

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.

(43)公開日 平成12年1月7日(2000.1.7)

(51) Int.Cl.	識別記号	F I	テーマコード(参考)
G 0 9 C 5/00		G 0 9 C 5/00	5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 C 0 7 6
H 0 4 N 1/387		H 0 4 N 1/387	

審査請求 有 請求項の数15 O L (全 27 頁)

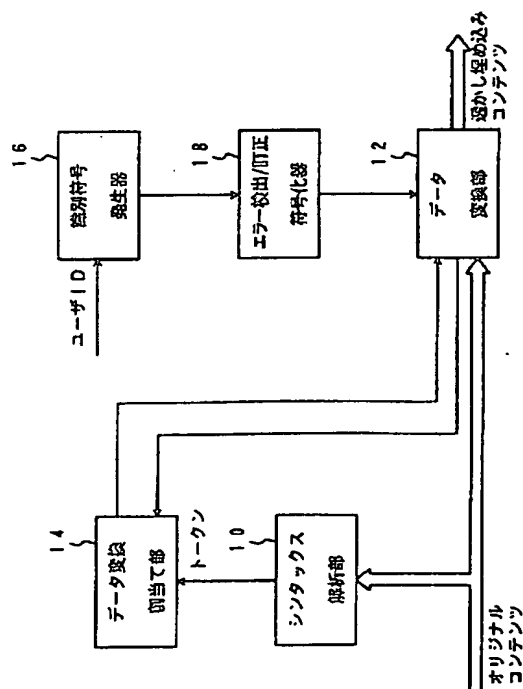
(21)出願番号	特願平10-122108	(71)出願人	396001360 株式会社ディジタル・ビジョン・ラボラト リーズ 東京都港区赤坂七丁目3番37号
(22)出願日	平成10年5月1日(1998.5.1)	(72)発明者	村谷 博文 東京都港区赤坂七丁目3番37号 株式会社 ディジタル・ビジョン・ラボラトリーズ内
(31)優先権主張番号	特願平10-108039	(74)代理人	100058479 弁理士 鈴江 武彦 (外5名)
(32)優先日	平成10年4月17日(1998.4.17)	Fターム(参考)	5B017 AA06 BA05 BA07 BB10 CA16 5C076 AA14 AA40 BA06
(33)優先権主張国	日本(JP)		

(54) 【発明の名称】 電子透かし埋め込み装置

(57) 【要約】

【課題】複数のユーザが結託して互いのデータを比較したとしても、透かしデータを改竄することが困難であるような透かしデータを埋め込む電子透かし埋め込み装置を提供することである。

【解決手段】デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を埋め込むことにより、たとえ複数のユーザが結託して、差分データを改竄して、自分達のデータ以外のデータに書換えたと思っても、改竄後のデータに自分達を示すデータが残ってしまい、結託が失敗する。



【特許請求の範囲】

【請求項1】 ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、

ユーザを識別する情報として、デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする電子透かし埋め込み装置。

【請求項2】 ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、

ユーザを識別する情報として、当該ユーザがデジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を用いることを特徴とする電子透かし埋め込み装置。

【請求項3】 ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、

ユーザを識別する情報として、デジタルデータを渡す可能性のあるユーザの各々に順位を付け、当該ユーザが各ユーザより順位が小さいか、等しいか、あるいは大きいかを表わす情報を用いることを特徴とする電子透かし埋め込み装置。

【請求項4】 ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、

ユーザを識別する情報として、デジタルデータを渡す可能性のあるユーザの各々に順位を付け、デジタルデータを渡す可能性のあるユーザの総数を N とし、 $N \leq p \times q$ となる互いに素の整数 p 、 q それぞれに対して、 p を法とした当該ユーザの順位 n の剰余が 0 から $p-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報と、 q を法とした当該ユーザの順位 n の剰余が 0 から $q-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報とをユーザを識別する情報として用いることを特徴とする電子透かし埋め込み装置。

【請求項5】 ユーザに渡すデジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、

対象を識別する情報として、全識別対象の中の任意の2つの識別対象の各々に対して、識別すべき対象がその対に含まれているか否かを表わす情報を発生することを特徴とする識別情報発生装置。

【請求項6】 ユーザに渡すデジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、

対象を識別する情報として、識別すべき対象が全識別対象の各々であるか否かを表わす情報を発生することを特

徴とする識別情報発生装置。

【請求項7】 ユーザに渡すデジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、

対象を識別する情報として、全識別対象の各々に順位を付け、識別すべき対象が各識別対象より順位が小さいか、等しいか、あるいは大きいかを表わす情報を発生することを特徴とする識別情報発生装置。

【請求項8】 デジタルデータを渡す可能性のあるユーザの総数を N とし、 $N \leq p \times q$ となる互いに素の整数 p 、 q それぞれに対して、 p を法とした当該ユーザの順位 n の剰余が 0 から $p-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報と、 q を法とした当該ユーザの順位 n の剰余が 0 から $q-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報とをユーザを識別する情報として用いることを特徴とする請求項7に記載の識別情報発生装置。

【請求項9】 デジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、

種々のデータ変換内容を記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、識別対象固有の情報に応じて、識別符号を発生する手段と、

前記データ割当て部から出力されたデータ変換内容と前記識別符号に応じて、デジタルデータの所定の部分を変更する識別符号埋め込み手段と、

を具備することを特徴とする識別符号埋め込み装置。

【請求項10】 デジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、

種々のデータ変換内容をその変化程度を表わすコストと共に記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、

データ変換後のデータの変化程度を累積する手段と、

識別対象固有の情報に応じて、識別符号を発生する手段と、

前記データ割当て部から出力されたデータ変換内容と前記識別符号に応じて、デジタルデータの所定の部分を変更する識別符号埋め込み手段と、

前記累積手段により、データの変化程度の累積値が所定の変化程度を超える場合、前記識別符号埋め込み手段の動作を禁止する手段とを具備することを特徴とする識別符号埋め込み装置。

【請求項11】 識別情報がユーザには知覚できないように埋め込まれているデジタルデータから識別情報を読み取る識別情報検出装置において、

デジタルデータの所定の位置に埋め込まれている識別符号を抽出する手段と、
抽出された識別符号を復号し、識別情報を求める手段と、
を具備することを特徴とする識別情報検出装置。

【請求項12】 請求項1に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、デジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、その部位が請求項1に記載の装置により埋め込まれた、そのユーザ対がこのデジタルデータに対応するユーザを含んでいることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が請求項1に記載の装置により埋め込まれた、そのユーザ対がこのデジタルデータに対応するユーザを含んでいることを表わす符号であると判定されたユーザ対を結託したユーザ対の候補と推定することを特徴とする識別情報読取方法。

【請求項13】 請求項2に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、デジタルデータから抽出された識別情報から各ユーザに対応する部位を読み取るステップと、その部位が請求項2に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザであることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が請求項2に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザであることを表わす符号であると判定されたユーザを結託したユーザの候補と推定することを特徴とする識別情報読取方法。

【請求項14】 請求項3に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、
1) デジタルデータから抽出された識別情報から各ユーザに対応する部位を順次読み取るステップと、
2) その部位が請求項3に記載の装置により埋め込まれた、そのユーザの順位がこのデジタルデータに対応するユーザの順位よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ1)、2)を繰り返すステップと、
3) 上記ステップ2)において、初めて現れたそれ以外の符号の次の部位から、各ユーザに対応する部位を順次読み取るステップと、
4) その部位が請求項3に記載の装置により埋め込まれた、そのユーザの順位がこのデジタルデータに対応するユーザの順位よりの大きいことを表す符号であるか、

それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ3)、4)を繰り返すステップと、

5) 抽出された識別情報の最後に到達するまで上記ステップ3)、4)、5)を繰り返すステップと、を具備し、

上記ステップ2)において、それ以外の符号が初めて現れた部位に対応するユーザを第一の結託ユーザ候補と推定し、

上記ステップ4)において、それ以外の符号が最後に現れた部位に対応するユーザを第二の結託ユーザ候補と推定することを特徴とする識別情報読取方法。

【請求項15】 請求項4に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、

1) デジタルデータから抽出された識別情報からpを法とするユーザのそれぞれに対応する部位を順次読み取るステップと、

2) その部位が、請求項4に記載の装置により埋め込まれた、pを法としたそのユーザの順位の剰余がpを法としたこのデジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ1)、2)を繰り返すステップと、

3) 上記ステップ2)において、初めて現れたそれ以外の符号を次の部位から、pを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

4) その部位が、請求項4に記載の装置により埋め込まれた、pを法としたそのユーザ順位の剰余がpを法としたこのデジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ3)、4)を繰り返すステップと、

5) 抽出された識別情報からpを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ3)、

4)、5)を繰り返すステップと、

6) 上記ステップ5)において、抽出された識別情報からpを法としたユーザ順位の剰余のすべての部位を読み取った後、その次の部位からqを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

7) その部位が、請求項4に記載の装置により埋め込まれた、qを法としたそのユーザの順位の剰余がqを法としたこのデジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ6)、7)を繰り返すステップと、

8) 上記ステップ7)において、初めて現れたそれ以外の符号を次の部位から、qを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

9) その部位が、請求項4に記載の装置により埋め込まれた、 q を法としたそのユーザ順位の剰余が q を法としたこのデジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ8)、9)を繰り返すステップと、

10) 抽出された識別情報から q を法としたユーザ順位のすべての部位を読み取るまで、上記ステップ8)、

9)、10)を繰り返すステップと、を具備し、上記ステップ2)において、それ以外の符号が初めて現れた部位に対応する p を法としたユーザ順位の剰余と、上記ステップ4)において、それ以外の符号が最後に現れた部位に対応する p を法としたユーザ順位の剰余と、上記ステップ7)において、それ以外の符号が初めて現れた部位に対応する q を法としたユーザ順位の剰余と、上記ステップ9)において、それ以外の符号が最後に現れた部位に対応する q を法としたユーザ順位の剰余とを組み合わせて構成される p を法とする剰余と q を法とする剰余の組に対して中国人剰余定理を適用して結託ユーザの候補を推定することを特徴とする識別情報読取方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は音声や画像等のデジタル著作物データに、そのデータの著作権者、ユーザ等に関するなんらかの情報（以下、透かしデータと称する）を著作権者、ユーザ等には知覚できない状態で埋め込み、隠し持たせる電子透かし埋め込み装置に関する。

【0002】

【従来の技術】デジタル技術の進歩により、映画、音楽、写真等の様々な著作物がデジタルデータ（デジタル著作物）として流通されている。そのため、デジタル著作物の著作権を巡る問題が深刻になってきている。近年、デジタル著作物の不正利用を防止するための技術として電子透かし技術が脚光を浴びてきている。この技術は、データの著作権者、提供者等の権利を保護するために、データの中に著作権者、提供者、ユーザに関する情報等を、ユーザには判別できない形で埋め込みし、不正利用があった場合に、そのユーザを特定できるようにするものである。この情報は電子透かし、ウォーターマーク、フィンガープリントと呼ばれる。

【0003】不正利用の防止についてさらに詳細に説明すると、著作権者はデジタル著作物を流通させる際に、ユーザを識別する透かしデータを埋め込んでおく。ユーザが著作権者の許可無く、デジタル著作物を無断で複製し、第三者に販売等を行うことがある。著作権者は不正と思われるコピーを発見したら、そのデータから透かしデータを検出し、無断複製、不正販売を行ったユーザを特定し、そのユーザにペナルティを課すことができる。透かしデータの種類や、デジタルデータへの埋

め込み箇所はユーザには分からないようになっているので、ユーザは透かしデータを取り除くことはできない。

【0004】しかし、透かしデータはユーザを識別する情報であり、ユーザ毎に異なるので、2人以上のユーザが結託すると、透かしデータの存在が簡単に分かってしまう欠点がある。すなわち、ユーザAとユーザBが互いのデータの差分をとると、ユーザAの透かしデータとユーザBの透かしデータそのものは識別できないものの、その埋め込み箇所は想定できる。そのため、ユーザはこれらの差分データに何らかの信号を加えることにより、透かしデータを改竄することができる。

【0005】例えば、デジタルデータがMPEG方式の動画である場合、3人のユーザをユーザA、B、Cとし、2ビットのデジタルデータで3人のユーザの識別のための透かし情報を埋め込む。ユーザAの識別符号を“10”、ユーザBの識別符号を“01”、ユーザCの識別符号を“11”とする。識別符号“00”はどのユーザも識別しない。これらの2ビットの識別符号の埋め込み方は、1ビット目は i 番目のフレームの (x, y) 画素の輝度データに埋め込み、その1ビット目のデータが“1”の場合は輝度データ V を $V+1$ とし、“0”の場合は輝度データ V を V のままとし、2ビット目は j 番目のフレームの (v, w) 画素の輝度データに埋め込み、その2ビット目のデータが“1”の場合は輝度データ V' を $V'+1$ とし、“0”の場合は輝度データ V' を V' のままとすることにより、埋め込む。

【0006】そのため、 i 番目のフレームの (x, y) 画素、 j 番目のフレームの (v, w) 画素の輝度データを調べるとユーザを特定できる。ユーザAの識別符号“10”は $(V+1, V')$ 、ユーザBの識別符号“01”は $(V, V'+1)$ である。

【0007】ユーザA、Bは互いのデータを比較して、 i 番目のフレームの (x, y) 画素、 j 番目のフレームの (v, w) 画素の輝度データが違うことが分かり、これらの輝度データにユーザを識別する透かしデータが埋め込まれていることが分かる。そして、これらの輝度データを書換えて、自分達を示す情報以外の識別情報に改竄したい。

【0008】

$(i; x, y) : (V+1, \text{または} V) \rightarrow V + \Delta V$
これは、 i 番目のフレームの (x, y) 画素の輝度データ $V+1$ 、または V を $V + \Delta V$ に書換えることを示す。

【0009】 $(j; v, w) : (V', \text{または} V' + 1) \rightarrow V' + \Delta V'$

これは、 j 番目のフレームの (v, w) 画素の輝度データ V' 、または $V' + 1$ を $V' + \Delta V'$ に書換えることを示す。

【0010】 $\Delta V, \Delta V'$ をどのように選ぶかを考える。

【0011】(イ) $\Delta V = 1, \Delta V' = 0$ これは、ユー

ザAの識別符号と同じである。

【0012】(ロ) $\Delta V = 0$ 、 $\Delta V' = 1$
これは、ユーザBの識別符号と同じである。

【0013】(ハ) $\Delta V = 1$ 、 $\Delta V' = 1$
これは、ユーザCの識別符号である。

【0014】(ニ) $\Delta V = 0$ 、 $\Delta V' = 0$
この識別符号が定義されておらず、誰も特定しない。

【0015】このため、ユーザA、Bは(イ)、(ロ)の場合は自分達を示す識別情報に書き換わってしまい、 ΔV 、 $\Delta V'$ をこれ以外のデータに書き換えればよいことが分かる。もちろん、ユーザA、Bは(ハ)、(ニ)の書換え後の識別情報が具体的には何を意味しているかを認識してはいないが、これらのように書換えると、自分達を示す識別情報を改竄できることが想像できる。

【0016】以上に述べた透かしデータの埋め込みは一例であって、透かしデータはデジタルデータに対するより一般的な変換操作として多様な埋め込みが可能である。

【0017】

【発明が解決しようとする課題】このように従来の電子透かし埋め込み技術は、ユーザを識別する透かしデータを当該ユーザには知覚できない状態で埋め込み、隠し持たせることができるが、複数のユーザが結託してデータを互いに比較することにより、透かしデータが埋め込まれている位置に関する情報を得ることができてしまい、透かしデータの偽造や消去を容易にするという欠点があった。

【0018】本発明の目的は、複数のユーザが結託して互いのデータを比較したとしても、埋め込まれている透かしデータに関する情報を十分に得ることができず、透かしデータを偽造や消去することが困難となるように、デジタルデータに、そのデータのユーザ等に関する透かしデータを埋め込み、隠し持たせる電子透かし埋め込み装置を提供することである。

【0019】

【課題を解決するための手段】上記課題を解決し目的を達成するために、本発明は以下に示す手段を用いている。

【0020】(1) ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする。

【0021】(2) ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、当該ユーザがデジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を用

いることを特徴とする。

【0022】(3) ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のあるユーザのの各々に順位を付け、当該ユーザが各ユーザより順位が小さいか、等しいか、あるいは大きいかを表わす情報を用いることを特徴とする。

【0023】(4) ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のあるユーザのの各々に順位を付け、デジタルデータを渡す可能性のあるユーザの総数をNとし、 $N \leq p \times q$ となる互いに素の整数p、qそれぞれに対して、pを法とした当該ユーザの順位nの剰余が0からp-1までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報と、qを法とした当該ユーザの順位nの剰余が0からq-1までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報とをユーザを識別する情報として用いることを特徴とする。

【0024】(5) ユーザに渡すデジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、対象を識別する情報として、全識別対象の中の任意の2つの識別対象の各々に対して、識別すべき対象がその対に含まれているか否かを表わす情報を発生することを特徴とする。

【0025】(6) ユーザに渡すデジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、対象を識別する情報として、識別すべき対象が全識別対象の各々であるか否かを表わす情報を発生することを特徴とする。

【0026】(7) ユーザに渡すデジタルデータに、ユーザには知覚できないように付加する識別情報を発生する識別情報発生装置において、対象を識別する情報として、全識別対象の各々に順位を付け、識別すべき対象が各識別対象より順位が小さいか、等しいか、あるいは大きいかを表わす情報を発生することを特徴とする。

【0027】(8) (7)に記載の識別情報発生装置において、デジタルデータを渡す可能性のあるユーザの総数をNとし、 $N \leq p \times q$ となる互いに素の整数p、qそれぞれに対して、pを法とした当該ユーザの順位nの剰余が0からp-1までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報と、qを法とした当該ユーザの順位nの剰余が0からq-1までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報とをユーザを識別する情報として用いることを特徴とする。

【0028】(9) デジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、そ

の意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容を記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、識別対象固有の情報に応じて、識別符号を発生する手段と、前記データ割当て部から出力されたデータ変換内容と前記識別符号に応じて、デジタルデータの所定の部分を変更する識別符号埋め込み手段と、を具備することを特徴とする識別符号埋め込み装置。

【0029】(10) デジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容をその変化程度を表わすコストと共に記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、データ変換後のデータの変化程度を累積する手段と、識別対象固有の情報に応じて、識別符号を発生する手段と、前記データ割当て部から出力されたデータ変換内容と前記識別符号に応じて、デジタルデータの所定の部分を変更する識別符号埋め込み手段と、前記累積手段により、データの変化程度の累積値が所定の変化程度を超える場合、前記識別符号埋め込み手段の動作を禁止する手段とを具備することを特徴とする識別符号埋め込み装置。

【0030】(11) 識別情報がユーザには知覚できないように埋め込まれているデジタルデータから識別情報を読み取る識別情報検出装置において、デジタルデータの所定の位置に埋め込まれている識別符号を抽出する手段と、抽出された識別符号を復号し、識別情報を求める手段と、を具備することを特徴とする。

【0031】(12) 請求項1に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、デジタルデータから抽出された識別情報から各ユーザに対応する部位を読み取るステップと、その部位が請求項1に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザを含んでいることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が請求項1に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザを含んでいることを表わす符号であると判定されたユーザ対を結託したユーザ対の候補と推定することを特徴とする。

【0032】(13) 請求項2に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、デジタルデータから抽出された識別情報から各ユーザに対応する部位を読み取るステップと、その部位が請求項2に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザであることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が請求項2に記載の装

置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザであることを表わす符号であると判定されたユーザを結託したユーザの候補と推定することを特徴とする。

【0033】(14) 請求項3に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、

1) デジタルデータから抽出された識別情報から各ユーザに対応する部位を順次読み取るステップと、

2) その部位が請求項3に記載の装置により埋め込まれた、そのユーザの順位がこのデジタルデータに対応するユーザの順位よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ1)、2)を繰り返すステップと、

3) 上記ステップ2)において、初めて現れたそれ以外の符号の次の部位から、各ユーザに対応する部位を順次読み取るステップと、

4) その部位が請求項3に記載の装置により埋め込まれた、そのユーザの順位がこのデジタルデータに対応するユーザの順位よりも大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ3)、4)を繰り返すステップと、

5) 抽出された識別情報の最後に到達するまで上記ステップ3)、4)、5)を繰り返すステップと、を具備し、上記ステップ2)において、それ以外の符号が初めて現れた部位に対応するユーザを第一の結託ユーザ候補と推定し、上記ステップ4)において、それ以外の符号が最後に現れた部位に対応するユーザを第二の結託ユーザ候補と推定することを特徴とする。

【0034】(15) 請求項4に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、

1) デジタルデータから抽出された識別情報からpを法とするユーザのそれぞれに対応する部位を順次読み取るステップと、

2) その部位が、請求項4に記載の装置により埋め込まれた、pを法としたそのユーザの順位の剰余がpを法としたこのデジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ1)、2)を繰り返すステップと、

3) 上記ステップ2)において、初めて現れたそれ以外の符号を次の部位から、pを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

4) その部位が、請求項4に記載の装置により埋め込まれた、pを法としたそのユーザ順位の剰余がpを法としたこのデジタルデータに対応するユーザ順位の剰余よりも大きいことを表す符号であるか、それ以外の符号で

あるかを判定し、それ以外の符号が現れるまで、上記ステップ3)、4)を繰り返すステップと、

5) 抽出された識別情報からpを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ3)、

4)、5)を繰り返すステップと、

6) 上記ステップ5)において、抽出された識別情報からpを法としたユーザ順位の剰余のすべての部位を読み取った後、その次の部位からqを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

7) その部位が、請求項4に記載の装置により埋め込まれた、qを法としたそのユーザの順位の剰余がqを法としたこのデジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ6)、7)を繰り返すステップと、

8) 上記ステップ7)において、初めて現れたそれ以外の符号を次の部位から、qを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

9) その部位が、請求項4に記載の装置により埋め込まれた、qを法としたそのユーザ順位の剰余がqを法としたこのデジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ8)、9)を繰り返すステップと、

10) 抽出された識別情報からqを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ8)、

9)、10)を繰り返すステップと、を具備し、上記ステップ2)において、それ以外の符号が初めて現れた部位に対応するpを法としたユーザ順位の剰余と、上記ステップ4)において、それ以外の符号が最後に現れた部位に対応するpを法としたユーザ順位の剰余と、上記ステップ7)において、それ以外の符号が初めて現れた部位に対応するqを法としたユーザ順位の剰余と、上記ステップ9)において、それ以外の符号が最後に現れた部位に対応するqを法としたユーザ順位の剰余とを組み合わせ構成されるpを法とする剰余とqを法とする剰余の組に対して中国人剰余定理を適用して結託ユーザの候補を推定することを特徴とする。

【0035】

【発明の実施の形態】(第1実施形態) 以下、図面を参照して本発明による電子透かし埋め込み装置の第1の実施形態を説明する。

【0036】図1は電子透かし埋め込み装置の第1実施形態の全体のブロック図である。著作物であるデジタルデータ(以下、オリジナルコンテンツと称する)がシンタックス解析部10、データ変換部12に供給される。ここで、コンテンツは複数の意味を持ったひとまとまりのデータから構成されている。以下、このひとまとまりのデータのことを本明細書ではトークンと称す

る。例えば、MPEGビデオの符号化では、トークンとして各種のヘッダーコードやVLCコードなどがある。各トークンがコンテンツ中のどの位置にあって、どういう値を持つかは、そのデータをシンタックス解析することによって分かる。シンタックス解析部10はオリジナルコンテンツをシンタックス解析することにより、トークンを求める。トークンに関する情報は、データ変換割当て部14に通知される。データ変換割当て部14はトークンに応じてデータ変換部12にデータ変換規則を通知する。

【0037】ユーザ固有のユーザIDが識別符号発生器16に供給され、当該ユーザ名を特定できる識別符号が発生され、エラー検出/訂正符号化器18に供給される。エラー検出/訂正符号化器18はユーザ識別符号をエラー検出/訂正符号化し、データ変換部12に供給する。なお、このエラー検出/訂正符号化器18は本発明の必須の構成ではなく、図2に示すように、省略しても構わない。

【0038】データ変換部12はデータ変換割当て部14から通知されたデータ変換指示に従って、コンテンツの所定のビットを識別符号に応じて操作することによりコンテンツに識別符号(電子透かし)を埋め込む。埋め込みの一例は、従来例と同様に、MPEG動画の場合は、i番目のフレームの(x、y)画素の輝度データVを、埋め込むデータが“1”の場合はV+1とし、埋め込むデータが“0”の場合はそのままとすることにより、埋め込むことが考えられる。

【0039】図3はデータ変換割当て部14の具体的な構成を示すブロック図である。データ変換割当て部14はデータ変換の種々の内容を記憶する状態遷移メモリ22と、コンテンツの現在の状態を記憶する状態バッファ26と、コスト評価規則を記憶するコスト評価規則メモリ28と、コスト累積部20と、これらを制御するコントローラ24とからなる。シンタックス解析部10からのトークンに関する情報はコントローラ24に供給される。コントローラ24にはデータ変換部12からの電子透かし埋め込み後のデータが供給されるとともに、コントローラ24はデータ変換部12へ状態遷移メモリ22から読み出したデータ変換内容を示すデータ変換指示を与える。状態遷移メモリ22には前提条件毎にデータ変換内容(データ埋め込み規則)、及び変換後の状態である遷移状態、コスト(透かしデータの埋め込みにより、画質等のコンテンツの質の変化、あるいはデータ長の大きな変化等が生じるか否かを判定するための評価基準)を記憶する。状態バッファ26には、データ変換(透かし埋め込み)処理が行われる毎に、選択されたデータ変換内容に応じた遷移状態がセットされる。コントローラ24はトークンに応じた前提条件を検索し、対応するデータ変換内容を読み出し、データ変換部12へ供給する。ただし、コストを考慮して、透かしデータの埋め込

みによりデータが大きく変化することが予想される場合には、データ変換を行わない。このためにコスト評価規則メモリ28が設けられ、メモリ28はコスト累積部20に累積されているコストと、状態遷移メモリ22の選択したデータ変換内容に対応するコストとを比較し、所定値以上のデータの変化が予想される場合は、データ変換を非実行とする。

【0040】データ変換部12は実際に変換したデータに関する情報をコントローラ24へ返送する。コントローラ24はそのデータを基にコストを計算し、コスト累積部20に累積コストを蓄積する。

【0041】なお、コストによるコンテンツの質の変化判断は本発明の必須の構成ではなく、コスト判断は、省略しても構わない。この場合は、図4に示すように、状態遷移メモリ22からコストの欄を省略し、コスト累積部20、コスト評価規則メモリ28を省略すればよい。

【0042】第1の実施形態は、従来技術のように、単にユーザが誰であることを示すだけではなく、デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする。

【0043】例えば、デジタルデータがMPEG方式の動画像である場合、3人のユーザをユーザA、B、Cとし、各ユーザがユーザA、Bの対に含まれるか否か、ユーザB、Cの対に含まれるか否か、ユーザA、Cの対に含まれるか否かを表わす3ビットの識別符号を埋め込む。ユーザA、Bの対に含まれる場合は1ビット目を“1”とし、ユーザB、Cの対に含まれる場合は2ビット目を“1”とし、ユーザA、Cの対に含まれる場合は3ビット目を“1”とし、それ以外は“0”とする。これらの3ビットの識別符号の埋め込み方は、従来例と同様に、1ビット目はf1番目のフレームの(x1, y1)画素の輝度データV1を、“1”ならばV1+1とし、“0”ならばそのままとし、第2、第3ビット目はf2、f3フレームの(x2, y2)画素、(x3, y3)画素の輝度データV2、V3を、“1”ならば+1とし、“0”ならばそのままとすることにより、埋め込むことができる。

【0044】このような輝度データの変換はデータ変換部12で行われる。

【0045】次に、このような識別符号が埋め込みされたコンテンツをユーザが著作権者に無断で不正にコピーして販売する場合を説明する。従来例と同様に、ユーザA、Bが結託して、互いのデータを比較して、識別符号を改竄することを試みる。ユーザA、Bは、両者の差分データであるf2フレームの(x2, y2)画素の輝度データV2、f3フレームの(x3, y3)画素の輝度データV3がユーザA固有の透かしデータ、またはユーザB固有の透かしデータの一部であると推定でき、これを次のように書換えようとする。

【0046】(f2; x2, y2) : (V2、またはV2+1) → V2 + ΔV2

これは、f2フレームの(x2, y2)画素の輝度データV2、またはV2+1をV2 + ΔV2に書換えることを示す。

【0047】(f3; x3, y3) : (V3、またはV3+1) → V3 + ΔV3

これは、f3フレームの(x3, y3)画素の輝度データV3、またはV3+1をV3 + ΔV3に書換えることを示す。

【0048】ΔV2、ΔV3をどのように選ぶかを考える。

【0049】(イ) ΔV2 = 1、ΔV3 = 0

これは、ユーザBに埋め込まれる識別符号と同じである。

【0050】(ロ) ΔV2 = 0、ΔV3 = 1

これは、ユーザAに埋め込まれる識別符号と同じである。

【0051】(ハ) ΔV2 = 1、ΔV3 = 1

これは、結託者はユーザA、B、Cの中にいるが、どの2人であるか特定できないことを示す。

【0052】(ニ) ΔV2 = 0、ΔV3 = 0

これは、結託者はユーザAとBであることを示す。

【0053】このため、従来例と同じ推論で、ユーザA、Bは(イ)、(ロ)の場合は自分達を示す識別情報に書き換わってしまい、ΔV1、ΔV3をこれ以外のデータに書換えればよいと判断する。そして、ΔV1、ΔV3を(ハ)、(ニ)のように書換えて、違法コピーを再配布する。しかし、従来例と異なり、(ニ)の場合は、結託者がユーザAとBであることが分かってしまう。(ハ)の場合は、結託者を特定できないが、識別符号をL回、すなわち、3L画素に埋め込んでおくと、L個の識別符号が偶然に全て(ハ)の状態になるのは、 $(1/2)^L$ の確率であり、現実的には十分有効である。

【0054】このように第1実施形態によれば、デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を埋め込むことにより、たとえ複数のユーザが結託して、差分データを改竄して、自分達のデータ以外のデータに書換えても、改竄後のデータに自分達の対を示すデータが残ってしまうので、結託が失敗に終わる。

【0055】なお、本発明は識別符号としては、ユーザ名を識別する情報に限らず、一般的な対象を識別する情報をユーザに渡すデジタルデータに、ユーザには知覚できないように付加する場合にも適用できる。例えば、ユーザにその存在は知覚できるが、その符号の意味を教えていない形で、メッセージの一部として授受することができる。また、ユーザ名の識別以外の情報としては、

利用の日付、日時、利用者端末の識別、デジタルデータの識別、デジタルデータの転送経路の識別、利用の条件の記述等としても利用できる。

【0056】図5は第1実施形態の識別符号の発生アルゴリズムを示す図である。このアルゴリズムは、ユーザ名識別符号以外の一般的な識別符号に対しても適用できる。ステップS2で、識別対象部分集合（デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対） p_1, p_2, \dots, p_{max} に便宜上の順序を与える（ $p_1 < p_2 < \dots < p_{max}$ ）。ステップS4で、識別対象であるユーザ u を特定する。ステップS6で、変数 i に1をセットし、codeの初期値としてビット長0の初期値をセットする。ステップS8で、当該ユーザ u が部分集合 p_i に含まれているか否かを判定する。含まれている場合は、ステップS10で識別符号のビットcode($u \in p_i$)（ $=1$ ：第1実施形態の場合）を発生し、今までの識別符号に接続する。含まれていない場合には、ステップS12で識別符号のビットcode($u \neq p_i$)

（ $=0$ ：第1実施形態の場合）を発生し、今までの識別符号に接続する。ステップS10、S12で発生される符号は1ビットに限らず、複数ビットでもよい。記号 \neq は集合に属さない（ \in の否定）を表わす。この後、ステップS14で変数 i が max （部分集合の総数）以上か否かを判定する。ノーの場合は、ステップS16で変数 i をインクリメント（+1）して、ステップS8に戻り、当該ユーザ u が次の部分集合 p_i に含まれているか否かを判定する。ステップS14でイエスの判定が得られた場合は、全ての部分集合 p_i に対して当該ユーザ u がその部分集合に含まれるか否かの判定が終了し、識別符号の各ビットの発生、接続が終了したとして、動作終了する。

【0057】図6は、不正コピーと思えるコンテンツが流通し、コンテンツから透かしデータを抽出し、不正を働いたであろうユーザを識別するために用いられる透かし抽出装置の一例である。透かしデータの埋め込み位置を知るために、図1の透かし埋め込み装置と同様に、オリジナルコンテンツがシンタックス解析部40に供給され、トークンに関する情報がデータ変換割当て部42に入力される。データ変換割当て部42はトークンから透かしデータの埋め込み位置と変換内容を示す変換内容情報を発生する。なお、オリジナルコンテンツ毎に透かし埋め込み位置と変換内容は決まっているので、変換内容情報はトークンから毎回求めなくても良く、一度求めておいて、コンテンツ毎にメモリ等に格納しておいて、読み出す構成にしても良い。その場合、シンタックス解析部40とデータ変換割当て部42の代わりにメモリを設けることになる。

【0058】透かし埋め込み済みコンテンツと、データ変換割当て部42からの変換内容情報とが識別符号抽出部44に供給される。識別符号抽出部44は変換内容情

報に応じてコンテンツから埋め込まれている識別符号を抽出する。抽出された識別符号はエラー検出／訂正復号器46を介して、識別符号復号器48に供給され、識別符号に応じてユーザIDが検出される。透かし埋め込み装置側にエラー検出／訂正符号化器18が設けられていない場合には、エラー検出／訂正復号器46は省略される。エラー検出／訂正復号器46が設けられない場合の透かし抽出装置を図7に示す。

【0059】図8は第1実施形態の識別符号復号器48のアルゴリズムを示す。ステップS202で、識別対象部分集合（デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対） p_1, p_2, \dots, p_{max} に埋め込み時と同じ順序を与える（ $p_1 < p_2 < \dots < p_{max}$ ）。ステップS204で、codeの初期値として入力された抽出符号をセットする。ステップS206で、変数 i に1をセットし、結託者のユーザ対の候補であるcandidate-pairsに全部のユーザ対の集合 $\{p_1, p_2, \dots, p_{max}\}$ をセットする。

【0060】ステップS208で、codeの先頭の符号が1か否かを判定する。1である場合は、すぐにステップS212へ進む。1ではない場合は、ステップS210でcandidate-pairsからユーザ対 p_i を取り除いてから、ステップS212へ進む。ステップS212では、変数 i が max （部分集合の総数）以上か否かを判定する。ノーの場合は、ステップS214で変数 i をインクリメント（+1）し、ステップS216でcodeを1ビット左へシフトし、ステップS208のcodeの先頭の符号の判定に戻る。ステップS212でイエスの判定が得られた場合は、動作終了する。この後、candidate-pairsに残っているユーザ対 P が結託者対であると推測される。

【0061】図8のアルゴリズムの特徴をまとめると、1）デジタルデータから抽出された識別符号から各ユーザ対 p_i に対応する部位を読み取り、2）その部位が図5のアルゴリズムで埋め込まれた符号code u （ $u \in p_i$ ）であるか、それ以外の符号であるかを判定し、3）上記2）において、code u （ $u \in p_i$ ）であると判定されたユーザ対 p_i を結託したユーザ対の可能性があると推測できる。

【0062】識別符号が L 回埋め込まれた場合は、上記のアルゴリズムを L 回行い、各アルゴリズムの実行時に、常にcandidate-pairsに残っているユーザ対 P が結託者対である可能性が高いと推測される。

【0063】第1実施形態ではユーザ数を N とすると、任意のユーザ対からなる部分集合の総数は全部で $N C 2$ となり、識別符号の符号量は N^2 のオーダーとなり、 $log 2 N$ のオーダーであった従来例に比べて、複数のユーザの結託には強いが、符号量が増える。

【0064】そこで、識別符号の符号量が増大すること無く、しかもユーザの結託による改竄に強い透かしデー

タ埋め込みの他の実施形態を説明する。他の実施形態の説明において第1の実施形態と同一部分は同一参照数字を付してその詳細な説明は省略する。他の実施形態の装置構成は第1実施形態と同じであるので、構成を示すブロック図、およびその説明は省略する。

【0065】(第2実施形態)第2の実施形態は、当該ユーザがデジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を論理積(記号 \cap で表わす)の形で接続して用いることを特徴とする。例えば、ユーザ u_i に対しては、ユーザ $u_1 \sim u_{i-1}$ ではなく、ユーザ u_i であり、かつユーザ $u_{i+1} \sim u_N$ ではないという論理的な意味を持つ次のようなデータを埋め込む。

【0066】 $\neg u_1 \cap \neg u_2 \cap \dots \cap \neg u_{i-1} \cap u_i \neg u_{i+1} \cap \neg u_{i+2} \cap \dots \cap \neg u_N$

ここで、 \neg は否定を表わし、 $\neg u_1$ はユーザ u_1 ではないということを示すデータである。

【0067】具体的に埋め込むデータの符号を上の論理式のAND(\cap)をとっている個々の項に対応して割り当てる。

【0068】 $\neg u_i \rightarrow \text{code}_i(\neg u_i)$

$u_i \rightarrow \text{code}_i(u_i)$

埋め込むべき識別符号は個々の項に割り当てた符号を接続(記号 \parallel で表わす)して作ることにする。接続の順序は本実施形態では本質とは無関係であるが、説明の便宜上、ここではユーザに対応する添え字の順序とする。

【0069】ユーザ u_1 に埋め込む識別符号:

$\text{code}_1(u_1) \parallel \text{code}_1(\neg u_2) \parallel \text{code}_1(\neg u_3) \parallel \dots \parallel \text{code}_1(\neg u_N)$

ユーザ u_2 に埋め込む識別符号は

$\text{code}_2(\neg u_1) \parallel \text{code}_2(u_2) \parallel \text{code}_2(\neg u_3) \parallel \dots \parallel \text{code}_2(\neg u_N)$

ユーザ u_3 に埋め込む識別符号は

$\text{code}_3(\neg u_1) \parallel \text{code}_3(\neg u_2) \parallel \text{code}_3(u_3) \parallel \dots \parallel \text{code}_3(\neg u_N) \dots$

ユーザ u_i に埋め込む識別符号は

$\text{code}_i(\neg u_1) \parallel \text{code}_i(\neg u_2) \parallel \text{code}_i(\neg u_3) \parallel \dots \parallel \text{code}_i(\neg u_{i-1}) \parallel \text{code}_i(u_i) \parallel \text{code}_i(\neg u_{i+1}) \parallel \dots \parallel \text{code}_i(\neg u_N) \dots$

ユーザ u_N に埋め込む識別符号は

$\text{code}_N(\neg u_1) \parallel \text{code}_N(\neg u_2) \parallel \text{code}_N(\neg u_3) \parallel \dots \parallel \text{code}_N(\neg u_{N-1}) \parallel \text{code}_N(u_N)$

ここで、例えば、 $\text{code}_i(u_j)$ は“1”、 $\text{code}_i(\neg u_j)$ は“0”とする。

【0070】図9は第2実施形態の識別符号の発生アルゴリズムを示す図である。このアルゴリズムも、ユーザ名識別符号以外の一般的な識別符号に対しても適用できる。ステップS22で、全識別対象(デジタルデータを渡す可能性のある全ユーザ) $u_1, u_2, \dots, u_{\max}$ に便宜上の順序を与える($u_1 < u_2 < \dots < u_{\max}$)。ステップS24で、識別対象であるユーザ u_i を

特定する。ステップS26で、変数 j に1をセットし、 code_i に初期値(ビット長:0)をセットする。ステップS28で、変数 j がユーザ u_i を示すパラメータ i と等しいか否かを判定する。等しい場合は、ステップS30で識別符号の1ビット $\text{code}_i(u_j)$ (=“1”)を発生し、今までの識別符号に接続する。等しくない場合には、ステップS32で識別符号の1ビット $\text{code}_i(\neg u_j)$ (=“0”)を発生し、今までの識別符号に接続する。この後、ステップS34で変数 j が \max (ユーザの総数)以上か否かを判定する。ノーの場合は、ステップS36で変数 j をインクリメント(+1)して、ステップS28に戻り、変数 j が i に等しいか否かを判定する。ステップS34でイエスの判定が得られた場合は、全てのユーザに対して当該ユーザ u_i がそのユーザに等しいか否かの判定が終了し、識別符号の各ビットの発生、接続が終了したとして、動作終了する。

【0071】次に、このような識別符号が埋め込みされたコンテンツをユーザが著作権者に無断で不正にコピーして販売する場合を説明する。ユーザ u_i と u_j が結託すると、ユーザ u_i のデータの中の $\text{code}_i(u_i)$ と $\text{code}_i(\neg u_j)$ がユーザ u_j のデータの中の $\text{code}_j(\neg u_i)$ と $\text{code}_j(u_j)$ と違うので、これらを書換えることを考える。

【0072】すなわち、 $\text{code}_i(u_i)$ と $\text{code}_i(\neg u_j)$ を code_i' に、 $\text{code}_j(\neg u_i)$ と $\text{code}_j(u_j)$ を code_j' に書換えることになるが、書き換えの態様は次の態様が考えられる。

【0073】(イ) $\text{code}_i' = \text{code}_i(u_i)$, $\text{code}_j' = \text{code}_i(\neg u_j)$

これは、ユーザ u_i に埋め込まれる識別符号と同じである。

【0074】(ロ) $\text{code}_i' = \text{code}_j(\neg u_i)$, $\text{code}_j' = \text{code}_j(u_j)$

これは、ユーザ u_j に埋め込まれる識別符号と同じである。

【0075】(ハ) $\text{code}_i' = \text{code}_i(u_i)$, $\text{code}_j' = \text{code}_j(u_j)$

これは、結託者はユーザ u_i と u_j がであることを示す。

【0076】(ニ) $\text{code}_i' = \text{code}_j(\neg u_i)$, $\text{code}_j' = \text{code}_i(\neg u_j)$

この場合は、結託者を特定できない。

【0077】(ホ) $\text{code}_i' \neq \text{code}_i(u_i) \neq \text{code}_j(\neg u_i)$, $\text{code}_j' = \text{****}$

これは、ユーザ u_i が結託に参加していることを示す。

【0078】(ヘ) $\text{code}_i' = \text{****}$, $\text{code}_j' \neq \text{code}_j(u_j) \neq \text{code}_i(\neg u_j)$

これは、ユーザ u_j が結託に参加していることを示す。

【0079】このため、従来例と同じ推論で、ユーザA、Bは(イ)、(ロ)の場合は自分達を示す識別情報

に書き換わってしまい、これ以外の書き換えを行えばよいと判断する。そして、(ハ)、(ニ)、(ホ)、

(ヘ)のように書換えて、違法コピーを再配布する。しかし、従来例と異なり、(ハ)の場合は、結託者がユーザ u_i と u_j がであることが分かってしまうし、

(ホ)、(ヘ)の場合も、ユーザ u_i 、または u_j が結託者の1人であることが分かってしまう。また、(ニ)の場合は結託者を特定できないが、第1実施形態と同様に識別符号をL回埋め込むことにより、L個の識別符号が偶然に全て(ニ)の状態になるのは、 $(1/4)^L$ の確率であり、現実的には十分有効である。

【0080】図10は第2実施形態の識別符号復号器48のアルゴリズムを示す。ステップS222で、識別対象(ユーザ) $u_1, u_2, \dots, u_{\max}$ に埋め込み時と同じ順序を与える($u_1 < u_2 < \dots < u_{\max}$)。ステップS224で、codeの初期値として入力された抽出符号をセットする。ステップS226で、変数 i に1をセットし、結託ユーザの候補の集合である集合candidatesに空集合 $\{\}$ をセットする。

【0081】ステップS228で、codeの先頭はある j に対する $code_j (\neg u_i)$ であるか否かを判定する。イエスの場合は、すぐにステップS232に進み、ノーの場合は、ステップS230で集合candidatesにユーザ u_i を加えてから、ステップS232に進む。ステップS232では、変数 i が \max (ユーザの総数)以上か否かを判定する。ノーの場合は、ステップS234で変数 i をインクリメント(+1)し、ステップS236でcodeを $code_j (\neg u_i)$ の長さ(ビット数)だけ左へシフトし、ステップS228のcodeの先頭の判定に戻る。ステップS232でイエスの判定が得られた場合は、動作終了する。この後、集合candidatesに含まれているユーザが結託者であると推測される。

【0082】図10のアルゴリズムをまとめると、1)デジタルデータから抽出された識別符号から各識別対象 u_i に対応する部位を読み取り、2)その部位が図9のアルゴリズムで埋め込まれた符号 $code_i (u_j)$ であるか、それ以外の符号であるかを判定し、3)上記2)で符号 $code_i (u_j)$ であると判定されたユーザを結託したユーザの可能性があると推測できる。

【0083】識別符号がL回埋め込まれた場合は、上記のアルゴリズムをL回繰り返し、各アルゴリズムの実行時に、candidatesに含まれているユーザが結託者である可能性が高いと推測される。

【0084】このように第2実施形態によれば、当該ユーザがデジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を論理積の形で接続した識別符号を埋め込むことにより、たとえ複数のユーザが結託して、差分データを改竄して、自分達のデータ以外のデータに書換えても、改竄後のデータに自分達が結託に関与したことを示すデータが残ってしまうので、結託が失敗

に終わる。

【0085】第2実施形態の識別符号の符号量はオーダNの量であり、第1実施形態より符号量を大幅に削減することができる。

【0086】(第3実施形態)第2実施形態は3人以上のユーザの結託には弱い。

【0087】ユーザ u_i, u_j, u_k が結託する場合を考える。

【0088】ユーザ u_i に埋め込む識別符号：

$\dots \parallel code_i (u_i) \parallel \dots \parallel code_i (\neg u_j) \parallel \dots \parallel code_i (\neg u_k) \parallel \dots$

ユーザ u_j に埋め込む識別符号：

$\dots \parallel code_j (\neg u_i) \parallel \dots \parallel code_j (u_j) \parallel \dots \parallel code_j (\neg u_k) \parallel \dots$

ユーザ u_k に埋め込む識別符号：

$\dots \parallel code_k (\neg u_i) \parallel \dots \parallel code_k (\neg u_j) \parallel \dots \parallel code_k (u_k) \parallel \dots$

ユーザ u_i, u_j のデータの差分データから $code_i (u_i)$ 、または $\neg u_i$ と $code_j (u_j)$ 、または $\neg u_j$ の部位 P_{ij} が特定できる。ただし、各点がどちらに属するのかは分からない。同様に、ユーザ u_j, u_k のデータの差分データから $code_j (u_j)$ 、または $\neg u_j$ と $code_k (u_k)$ 、または $\neg u_k$ の部位 P_{jk} が特定できる。ただし、各点がどちらに属するのかは分からない。

【0089】これらの部分集合から、次のようにして u_i, u_j, u_k それぞれの部位 P_i, P_j, P_k が特定できる。

【0090】

$$\begin{aligned} & P_{i,j} \cap / P_{j,k} \rightarrow \\ & \{code_i (u_i, \text{または} \neg u_i) \text{の部位}\} \\ & P_i \\ & = P_{i,j} - P_{j,k} \end{aligned}$$

ここで、記号「/」は補集合を表わす。例えば、 P がデータ中のある部位とすると、 $/P$ はデータ中の P 以外の部分である。

【0091】

$$\begin{aligned} & P_{j,k} \cap / P_{i,j} \rightarrow \\ & \{code_k (u_k, \text{または} \neg u_k) \text{の部位}\} \\ & P_k \\ & = P_{j,k} - P_{i,j} \\ & P_{i,j} \cap / P_i \rightarrow \\ & \{code_i (u_i, \text{または} \neg u_i) \text{の部位}\} \\ & P_i \\ & = P_{i,j} - P_i \end{aligned}$$

この結果、次のことが分かる。

【0092】 u_i の埋め込みデータの P_i の部分は $code_i (u_i)$ を表わす。 u_i の埋め込みデータの P_i の部分は $code_i (\neg u_i)$ を表わす。これにより、 $code_i (u_i)$ 、 $code_i (\neg u_i)$ が分かってしまう。

【0093】同様にして、 $code_j (u_j)$ 、 $code_j (\neg$

u_j)、code k (u_k)、code k ($\neg u_k$) が分かってしまう。

【0094】このため、結託者はcode i ($\neg u_i$)、code j ($\neg u_j$)、code k ($\neg u_k$) を P_i 、 P_j 、 P_k に書き込むと、誰のものでもないデータを生成できてしまう。

【0095】このような3人以上の結託に対しても強くするために、ユーザの集合に次のように整列順序を付す。これは、コンテンツの提供者が決めればよい。

【0096】 $u_1 < u_2 < \dots < u_{i-1} < u_i < u_{i+1} < \dots < u_{j-1} < u_j < u_{j+1} < \dots < u_N$

順序を付す理由は、結託に加わったユーザを最小値、最大値とする部分集合を特定できるようにすることである。例えば、部分集合 $u_i < u_{i+1} < \dots < u_{j-1} < u_j$ が特定されると、結託に加わったユーザはユーザ u_i 、 u_j 、その他であることが分かる。

【0097】ユーザ u_1 に埋め込む識別符号：

code 1 (u_1) \parallel code 1 ($\neg u_2$) \parallel code 1 ($\neg u_3$) $\parallel \dots \parallel$ code 1 ($\neg u_N$)

ユーザ u_2 に埋め込む識別符号は

code 2 ($\neg u_1$) \parallel code 2 (u_2) \parallel code 2 ($\neg u_3$) $\parallel \dots \parallel$ code 2 ($\neg u_N$)

ユーザ u_3 に埋め込む識別符号は

code 3 ($\neg u_1$) \parallel code 3 ($\neg u_2$) \parallel code 3 (u_3) $\parallel \dots \parallel$ code 3 ($\neg u_N$) \dots

ユーザ u_i に埋め込む識別符号は

code i ($\neg u_1$) \parallel code i ($\neg u_2$) \parallel code i ($\neg u_3$) $\parallel \dots \parallel$ code i ($\neg u_{i-1}$) \parallel code i (u_i) \parallel code i ($\neg u_{i+1}$) $\parallel \dots \parallel$ code i ($\neg u_N$) \dots

code 1 (u_1) \neq code 2 ($\neg u_1$) = code 3 ($\neg u_1$) = \dots
= code N ($\neg u_1$)

code 1 ($\neg u_2$) \neq code 2 (u_2) \neq code 3 ($\neg u_2$) = \dots
= code N ($\neg u_2$)

code 1 ($\neg u_3$) = code 2 ($\neg u_3$) \neq code 3 (u_3) \neq code 4 ($\neg u_3$)
= \dots = code N ($\neg u_3$)

\dots

ここで、等しいcodeは同一の変数を用いると、全部で3つの変数 a 、 b 、 c 用いて、次のように識別符号を表わ

ユーザ u_1 に埋め込む識別符号： $a^{(1)}$ $b^{(2)}$ $b^{(3)}$ $\dots \dots \dots b^{(N)}$

ユーザ u_2 に埋め込む識別符号： $c^{(1)}$ $a^{(2)}$ $b^{(3)}$ $\dots \dots \dots b^{(N)}$

ユーザ u_i に埋め込む識別符号： $c^{(1)}$ $c^{(2)}$ $c^{(3)}$ $\dots a^{(i)}$ $\dots \dots b^{(N)}$

ユーザ u_N に埋め込む識別符号： $c^{(1)}$ $c^{(2)}$ $c^{(3)}$ $\dots \dots c^{(N-1)}$ $a^{(N)}$

図11は第3実施形態の識別符号の発生アルゴリズムを示す図である。このアルゴリズムも、ユーザ名識別符号以外の一般的な識別符号に対しても適用できる。ステップS42で、全識別対象（デジタルデータを渡す可能性のある全ユーザ） u_1 、 u_2 、 \dots u_N に順序を与える ($u_1 < u_2 < \dots < u_N$)。ステップS44で、識別対象であるユーザ u_i を特定する。ステップS46で、変数 j に1をセットし、codeに初期値（ビット長：0）を

ユーザ u_N に埋め込む識別符号は

code N ($\neg u_1$) \parallel code N ($\neg u_2$) \parallel code N ($\neg u_3$) $\parallel \dots \parallel$ code N ($\neg u_{N-1}$) \parallel code N (u_N)

一般的に、ユーザ u_i に埋め込む識別符号において、code i (u_i) より前のcode i ($\neg u_1$) \parallel code i ($\neg u_2$) $\parallel \dots \parallel$ code i ($\neg u_{i-1}$) は、ここには結託者はいない (i 番目より順位の小さいユーザは結託に参加していない) ことを示す。同様に、code i (u_i) より後のcode i ($\neg u_{i+1}$) $\parallel \dots \parallel$ code i ($\neg u_N$) も、ここには結託者はいない (i 番目より順位の大きいユーザは結託に参加していない) ことを示す。すなわち、第3実施形態では、対象を識別する情報として、全識別対象の各々に順位を付け、識別すべき対象が各識別対象より順位が小さいか、等しいか、あるいは大きいかを表わす情報を用いる。

【0098】ユーザ u_i 、 u_j に埋め込む識別符号に関しては、場所によって符号の意味が異なるものには、異なる符号を割り当てる。例えば、 i 番目のデータは、ユーザ u_i に埋め込む識別符号に対しては、このデータは u_i のものであることを意味し、ユーザ u_j に埋め込む識別符号に対しては、 u_i より小さいユーザに結託者はいないことを意味する。また、 k ($i < k < j$) 番目のデータは、ユーザ u_i に埋め込む識別符号に対しては、 u_k より大きいユーザに結託者はいないことを意味し、ユーザ u_j に埋め込む識別符号に対しては、 u_k より小さいユーザに結託者はいないことを意味する。

【0099】これを考慮すると、次のような符号を割り当てる可以考虑。

【0100】

code 1 (u_1) \neq code 2 ($\neg u_1$) = code 3 ($\neg u_1$) = \dots

= code N ($\neg u_1$)

code 1 ($\neg u_2$) \neq code 2 (u_2) \neq code 3 ($\neg u_2$) = \dots

= code N ($\neg u_2$)

code 1 ($\neg u_3$) = code 2 ($\neg u_3$) \neq code 3 (u_3) \neq code 4 ($\neg u_3$)

= \dots = code N ($\neg u_3$)

\dots

することができる。

【0101】

ユーザ u_1 に埋め込む識別符号： $a^{(1)}$ $b^{(2)}$ $b^{(3)}$ $\dots \dots \dots b^{(N)}$

ユーザ u_2 に埋め込む識別符号： $c^{(1)}$ $a^{(2)}$ $b^{(3)}$ $\dots \dots \dots b^{(N)}$

ユーザ u_i に埋め込む識別符号： $c^{(1)}$ $c^{(2)}$ $c^{(3)}$ $\dots a^{(i)}$ $\dots \dots b^{(N)}$

ユーザ u_N に埋め込む識別符号： $c^{(1)}$ $c^{(2)}$ $c^{(3)}$ $\dots \dots c^{(N-1)}$ $a^{(N)}$

セットする。

【0102】ステップS48で、変数 j がユーザ u_i を示すパラメータ i と等しいか否かを判定する。等しい場合は、ステップS50で識別符号の1ビット $a^{(i)}$ を発生し、今までの識別符号に接続する。等しくない場合には、ステップS52で変数 j がユーザ u_i を示すパラメータ i より小さいか否かを判定する。小さい場合は、ステップS54で識別符号の1ビット $c^{(j)}$ を発生し、今

までの識別符号に接続する。小さくない場合には、ステップS56で、識別符号の1ビット $b(i)$ を発生し、今までの識別符号に接続する。

【0103】この後、ステップS58で変数 j が N （ユーザの総数）以上か否かを判定する。ノーの場合は、ステップS60で変数 j をインクリメント（+1）して、ステップS48に戻り、変数 j が i に等しいか否かを判定する。ステップS58でイエスの判定が得られた場合

ユーザ u_i に埋め込む識別符号：

$c(i) \dots c(i-1) \ a(i) \ b(i+1) \dots b(N)$

ユーザ u_j に埋め込む識別符号：

$c(i) \dots \dots c(j-1) \ a(j) \ b(j+1) \dots b(N)$

ユーザ u_k に埋め込む識別符号：

$c(i) \dots \dots c(k-1) \ a(k) \ b(k+1) \dots b(N)$

3人のユーザが結託に成功するためには次のような識別符号が得られる必要がある。

$c(i) \dots c(i-1) \ * (i) \ * (i+1) \dots * (k-1) \ * (k) \ b(k+1) \dots b(N)$

この $* (i) \ * (i+1) \dots * (k-1) \ * (k)$ の部分集合が結託者を特定するので、最小値 $* (i)$ が $a(i)$ ではユーザ u_i が結託に参加していることが分かってしまう。そのため、 $* (i) = c(i)$ としてユーザ u_i は結託に参加していないことにしないとイケない。また、 $* (i) = b(i)$ 、その他のコードではユーザ u_i が結託に参加していることになってしまう。ユーザ u_i の識別符号の部位 P_i が特定できれば、ユーザ u_k のデータから、 $* (i) = c(i)$ とするのは容易である。しかし、特定できるのは、 $P_i \dots P_{j-1}$ （ $P_{ij} - P_{jk}$ ）という全体であり、部位 P_i は特定できない。

【0107】同様に、最大値 $* (k)$ が $a(k)$ ではユーザ u_k が結託に参加していることが分かってしまう。そのため、 $* (k) = b(k)$ としてユーザ u_k は結託に参加していないことにしないとイケない。また、 $* (k) = c(k)$ 、その他のコードではユーザ u_k が結託に参加していることになってしまう。ユーザ u_k の識別符号の部位 P_k の部分が特定できれば、ユーザ u_i のデータから、 $* (k) = b(k)$ とするのは容易である。しかし、特定できるのは、 $P_{j+1} \dots P_k$ （ $P_{jk} - P_{ij}$ ）という全体であり、部位 P_k は特定できない。

【0108】ランダムな操作により $* (i) = c(i)$ 、かつ $* (k) = b(k)$ とするには偶然に頼るしかなく、それその確率を $p(i)$ 、 $p(k)$ とすると、結託が成功する確率は $p(i) \times p(k)$ となり、一般に、 $p(i) \leq 1/2$ 、 $p(k) \leq 1/2$ であって、特に、 $c(i)$ と $b(k)$ の符号長がある程度長い場合には、 $p(i)$ と $p(k)$ は1より十分小さいので、結託が成功する確率は小さいと言える。さらに、上記実施形態と同様に、識別情報を L 回埋め込むことにより、この確率を $(p(i) \times p(k))^L$ と、さらに小さくすることができる。

【0109】図12は第3実施形態の識別符号復号器48のアルゴリズムを示す。ステップS242で、識別対

は、全てのユーザに対して当該ユーザ u_i がそのユーザに等しいか否かの判定が終了し、識別符号の各ビットの発生、接続が終了したとして、動作終了する。

【0104】次に、このような識別符号を埋め込むことにより、3人のユーザ u_i 、 u_j 、 u_k が結託したとしても、結託が成功しない理由を説明する。

【0105】

【0106】

象（ユーザ） u_1, u_2, \dots, u_N に埋め込み時と同じ順序を与える（ $u_1 < u_2 < \dots < u_N$ ）。ステップS244で、変数 i に1をセットし、codeの初期値として入力された抽出符号をセットし、第1の結託者の候補であるcandidate 1に1をセットし、第2の結託者の候補であるcandidate 2に1をセットする。ステップS246で、codeの先頭が $c(i)$ であるか否かを判定する。イエスの場合は、ステップS248で変数 i をインクリメント（+1）し、ステップS250で第1の結託者の候補であるcandidate 1、及び第2の結託者の候補であるcandidate 2をそれぞれインクリメント（+1）する。ステップS252でcodeを $c(i)$ の長さだけ左へシフトし、ステップS246のcodeの先頭の判定に戻る。ここで、 $c(i)$ の長さを $|c(i)|$ と表わし、 $|a(i)| = |b(i)| = |c(i)|$ とする。ステップS246でノーの判定が得られた場合は、ステップS254で変数 i をインクリメント（+1）し、codeを $c(i)$ の長さだけ左へシフトし、ステップS256で、codeの先頭が $b(i)$ であるか否かを判定する。ノーの場合は、ステップS258で第2の結託者の候補であるcandidate 2に変数 i を代入し、ステップS254へ戻る。ステップS260でイエスの判定が得られた場合は、動作終了する。この後、candidate 1、candidate 2が結託者の中の2人であると推測される。

【0110】図12のアルゴリズムの特徴をまとめると、1）デジタルデータから抽出された識別符号を先頭から順次、各識別対象 u_i に対応する部位を読み取り、2）その部位が、図11のアルゴリズムで埋め込まれた符号 $c(i)$ であるか、それ以外の符号であるかを判定し、 $c(i)$ 以外の符号が現われるまで、上記1）、2）を繰り返し、3）上記2）において初めて $c(i)$ 以外の符号が現われたときの、 i を結託ユーザの候補の一人であると判定し、4）上記2）において初めて現われ

たc(i)以外の符号の次の部位から、各識別対象u_iに対応する部位を読み取り、5)その部位が、図11のアルゴリズムで埋め込まれた符号b(i)であるか、それ以外の符号であるかを判定し、b(i)以外の符号が現われるまで、上記4)、5)を繰り返し、6)上記5)においてb(i)以外の符号が現われたときの、iが結託ユーザのもう一人の候補であると「仮に」判定し、7)抽出された識別符号の最後に到達するまで上記4)、5)、6)を繰り返し、8)抽出された識別符号の最後に到達した時点での結託ユーザのもう一人の候補として「仮に」判定されているユーザをもう一人の結託ユーザであると判定する。

【0111】識別符号がL回埋め込まれた場合は、上記のアルゴリズムをL回行い、各アルゴリズムの実行時に、candidate 1、candidate 2が結託者である可能性が高いと推測される。

【0112】第3実施形態の識別符号の符号量もオーダNの量であり、第1実施形態より符号量を大幅に削減することができる。

【0113】結託攻撃に対する電子透かしの従来例として、「結託攻撃に強い電子透かし法」鈴置昌宏等、SCI S'97 The 1997 Symposium on Cryptography and Information Security と "Collusion-Secure Fingerprinting for Digital Data", D. Boneh and J. Shaw, Advances in Cryptology Proceedings of CRYPTO'95, pp257-270(1994)があるが、鈴置等の例は、a=00、b=10、c=01に相当し、Boneh et al.の例は、a、b、cはL(任意の正整数)ビットであり、a a=b=00...0(全て0)、c=11...1(全て1)に相当する。すなわち、第3実施形態はこれらの方法よりも、一般的な符号化であると言える。

【0114】(第4実施形態)さらに、符号量を削減する実施形態を説明する。この実施形態は、中国人剰余定理を応用するものである。中国人剰余定理とは、互いに素な整数p₁、p₂、...p_k(これらの整数はn≤p₁×p₂×...×p_kという関係を満たす)があった時、n₁=n mod p₁、n₂=n mod p₂、...n_k=n mod p_kというn₁、n₂、...n_kからnが一意的に求められるという定理である。これを応用(N≤p×qとする)すると、1~pの中のr番目と、1~qの中のs番目のユーザを特定することにより、第3実施形態のユーザ数Nの全ユーザの集合中のn番目のユーザを特定することができる。ユーザ数pとqの2つの集合中のそれぞれr(=n mod p)、s(=n mod q)番目のユーザを特定する識別符号の方がユーザ数Nの全ユーザの集合中のn番目のユーザを特定する識別符号よりも符号量が少なくて済む。

【0115】第4実施形態において、N≤p×qとなる互いに素な整数p、qを定義し、ユーザを特定するパラメータi(i=1~N)の代わりに、パラメータr(1

~p)およびs(1~q)により各ユーザを特定する。説明の便宜上、p=7、q=5とする。

【0116】ユーザu₁に埋め込む識別符号：

a(1) b(2) b(3) b(4) b(5) b(6) b(7) a(1)
b(2) b(3) b(4) b(5)

ユーザu₂に埋め込む識別符号：

c(1) a(2) b(3) b(4) b(5) b(6) b(7) c(1)
a(2) b(3) b(4) b(5)...

ユーザu₆に埋め込む識別符号：

c(1) c(2) c(3) c(4) c(5) a(6) b(7) a(1)
b(2) b(3) b(4) b(5)

ユーザu₇に埋め込む識別符号：

c(1) c(2) c(3) c(4) c(5) c(6) a(7) c(1)
a(2) b(3) b(4) b(5)

ユーザu₈に埋め込む識別符号：

a(1) b(2) b(3) b(4) b(5) b(6) b(7) c(1)
c(2) a(3) b(4) b(5)...

上の符号の前半部分*(1)* (2)* (3)* (4)* (5)* (6)* (7)はrに関する符号部分code_rであり、後半部分*(1)* (2)* (3)* (4)* (5)* (6)* (7)はsに関する符号部分code_sである。それぞれ、符号aの位置がr、sの値を示す。なお、rに関する符号部分に含まれる符号a、b、cと後半部分に含まれる符号a、b、cは同じ物である必要は無く、後半部分に含まれる符号はd、e、fでもよい。

【0117】図13、図14は第4実施形態の識別符号の発生アルゴリズムを示す図である。このアルゴリズムも、ユーザ名識別符号以外の一般的な識別符号に対しても適用できる。ステップS64で、全識別対象(デジタルデータを渡す可能性のある全ユーザ)u₁、u₂、...u_N(u₁<u₂<...<u_N)に順序を与える。ステップS66で、識別対象であるユーザu_iを特定する。ステップS68で、N≤p×qを満たす互いにその整数p、qを求める。ステップS70で、変数jに1をセットし、code_rに初期値(ビット長：0)をセットする。ステップS72で、変数jがi mod pと等しいか否かを判定する。等しい場合は、ステップS74で識別符号code_rの1ビットa(i)を発生し、今までの識別符号code_rに接続する。等しくない場合には、ステップS76で変数jがi mod pより小さいか否かを判定する。小さい場合は、ステップS78で識別符号code_rの1ビットc(i)を発生し、今までの識別符号code_rに接続する。小さい場合には、ステップS80で、識別符号code_rの1ビットb(i)を発生し、今までの識別符号に接続する。

【0118】この後、ステップS82で変数jがp以上か否かを判定する。ノーの場合は、ステップS84で変数jをインクリメント(+1)して、ステップS72に戻り、変数jがi mod pに等しいか否かを判定する。ステップS82でイエスの判定が得られた場合は、識別符

号code_rの全ビット(pビット)の発生、接続が終了したとして、code_sの発生に移る。

【0119】ステップS86で、変数jに1をセットし、code_sに初期値(ビット長:0)をセットする。ステップS88で、変数jがi mod qと等しいか否かを判定する。等しい場合は、ステップS90で識別符号code_sの1ビットa⁽ⁱ⁾を発生し、今までの識別符号code_sに接続する。等しくない場合には、ステップS92で変数jがi mod qより小さいか否かを判定する。小さい場合は、ステップS94で識別符号code_sの1ビットc⁽ⁱ⁾を発生し、今までの識別符号code_sに接続する。小さくない場合には、ステップS96で、識別符号code_sの1ビットb⁽ⁱ⁾を発生し、今までの識別符号に接続する。

【0120】この後、ステップS98で変数jがq以上か否かを判定する。ノーの場合は、ステップS100で変数jをインクリメント(+1)して、ステップS88に戻り、変数jがi mod qに等しいか否かを判定する。ステップS98でイエスの判定が得られた場合は、識別符号code_sの全ビット(qビット)の発生、接続が終了したとして、ステップS102でcode_rとcode_sとを接続し、識別符号の発生を終了する。

【0121】このように識別符号を2つの部分に分けたことにより、符号量はNのオーダではなく、(pのオーダ)+(qのオーダ)となる。ここで、 $p \approx q$ とすると、 $p^2 \approx q^2 \approx N$ となり、識別符号の長さは $N^{1/2}$ のオーダとなる。

【0122】なお、第4実施形態においては、rとしてはr₁とr₂が求められ、sとしてはs₁とs₂が求められるので、結託者はr₁とs₁とで決まる1名とr₂とs₂とで決まる1名か、あるいはr₁とs₂とで決まる1名とr₂とs₁とで決まる1名であるのか特定できない。そこで、この一方を特定するためには、さらに次のような第3の整数tを導入する必要がある。 $n \bmod t = u$ とする。

【0123】 $N = p \times q$ 、
 $N \leq p \times t$ 、
 $N \leq q \times t$

これから、rとしてはr₁とr₂が求められ、sとしてはs₁とs₂が求められ、tとしてはt₁とt₂が求められる。rとsから結託者はr₁とs₁とで決まる1名とr₂とs₂とで決まる1名である(これをn₁、n₂とする)か、あるいはr₁とs₂とで決まる1名とr₂とs₁とで決まる1名である(これをn₁'、n₂'とする)ことが分かる。sとtから結託者はs₁とt₁とで決まる1名とs₂とt₂とで決まる1名である(これをm₁、m₂とする)か、あるいはs₁とt₂とで決まる1名とs₂とt₁とで決まる1名である(これをm₁'、m₂'とする)ことが分かる。これら4通りの候補:

(n₁、n₂)、(n₁'、n₂')、(m₁、

m₂)、(m₁'、m₂')の中から一致するものが結託者であると判定する。

【0124】第4実施形態の識別符号復号器48のアルゴリズムは、図12に示した第3実施形態のアルゴリズムを整数p、qに対してそれぞれ実行すればよい。このアルゴリズムを図15、図16に示す。ステップS272で、識別対象(ユーザ)u₁、u₂、…u_Nに埋め込み時と同じ順序を与える(u₁<u₂<…<u_{max})とともに、埋め込み時と同じ整数p、qを与える。ステップS274で、変数iに1をセットし、codeの初期値として入力された抽出符号をセットし、第1の結託者の候補であるcandidate - p₁に1をセットし、第2の結託者の候補であるcandidate - p₂に1をセットする。ステップS276で、codeの先頭の符号がc⁽ⁱ⁾であるか否かを判定する。イエスの場合は、ステップS278で変数iをインクリメント(+1)し、ステップS280で第1の結託者の候補であるcandidate - p₁、及び第2の結託者の候補であるcandidate - p₂をそれぞれインクリメント(+1)する。ステップS282でcodeをc⁽ⁱ⁾の長さだけ左へシフトし、ステップS276のcodeの先頭の符号の判定に戻る。ステップS276でノーの判定が得られた場合は、ステップS284で変数iをインクリメント(+1)し、codeをc⁽ⁱ⁾の長さだけ左へシフトし、ステップS286で、codeの先頭の符号がb⁽ⁱ⁾であるか否かを判定する。ノーの場合は、ステップS288で第2の結託者の候補であるcandidate - p₂にiをセットし、ステップS284へ戻る。ステップS286でイエスの判定が得られた場合は、ステップS290で、変数iがp以上であるか否かを判定する。

【0125】ノーの場合は、ステップS284に戻り、イエスの場合は、ステップS292で、第1の結託者の候補であるcandidate - q₁に1をセットし、第2の結託者の候補であるcandidate - q₂に1をセットする。ステップS294で、変数iをインクリメント(+1)し、ステップS296で、codeの先頭の符号がc⁽ⁱ⁾であるか否かを判定する。イエスの場合は、ステップS298で、変数iをインクリメント(+1)し、ステップS300で第1の結託者の候補であるcandidate - q₁、及び第2の結託者の候補であるcandidate - q₂をそれぞれインクリメント(+1)する。ステップS302でcodeをc⁽ⁱ⁾の長さだけ左へシフトし、ステップS296のcodeの先頭の符号の判定に戻る。ステップS296でノーの判定が得られた場合は、ステップS304で変数iをインクリメント(+1)し、codeをc⁽ⁱ⁾の長さだけ左へシフトし、ステップS306で、codeの先頭の符号がb⁽ⁱ⁾であるか否かを判定する。ノーの場合は、ステップS308で第2の結託者の候補であるcandidate - q₂にiをセットし、ステップS304へ戻る。ステップS306でイエスの判定が得られた場合は、ステップS310で、変数iがp+q以上であるか

否か判定する。ノーの場合は、ステップS304に戻り、イエスの場合は、ステップS312で、(candidate - p1, candidate - q1), (candidate - p2, candidate - q2), (candidate - p1, candidate - q2), (candidate - p2, candidate - q1) に対して中国人剰余定理を適用し、結託ユーザの候補の順位 n を計算し、決定する。

【0126】上述した第4実施形態は、2つの整数 p 、 q の組み合わせを用いたが、中国人剰余定理の通り、 k 個の整数 p_1, p_2, \dots, p_k を用いることもできる。この場合、 $v_i = N \bmod p_i$ とし、 v_i から n を求めるアルゴリズムを図17に示す。

【0127】ステップS120で変数 i に1をセットする。ステップS122で $y_i = \text{inv}((N/p_i) \bmod p_i, p_i)$ を求める。ステップS124で変数 i が k 以上であるか否か判定する。ノーの場合は、ステップS126で変数 i をインクリメント(+1)し、ステップS122を再度実行する。ステップS124でイエスの判定が得られたら、ステップS128で x に初期値0をセットし、ステップS130で変数 i に再度0をセットする。ステップS132で $x = x(x + (N/p_i) \cdot y_i \cdot v_i) \bmod N$ を計算する。ステップS134で変数 i が k 以上であるか否か判定する。ノーの場合は、ステップS136で変数 i をインクリメント(+1)し、ステップS132を再度実行する。ステップS134でイエスの判定が得られたら、ステップS138で x をユーザ n を特定する情報として出力する。

【0128】本発明は上述した実施形態に限定されず、種々変形して実施可能である。例えば、上記実施形態は、デジタルデータを配布する提供者側で識別符号を生成するとともに、デジタルデータに埋め込んだが、識別符号の生成と、埋め込みとを分離してもよい。すなわち、識別符号は、信頼できる第3者が行い、生成した識別符号をクライアントであるデジタルデータ提供者に配布し、提供者側では、配布された識別符号をそのまま埋め込む。

【0129】このようにすると、識別符号を電子透かし以外の目的で利用できる。例えば、ユーザにその存在が知覚できるが、その符号の意味を教えていない形で、メッセージの一部として授受することができる。また、ユーザ名の識別以外の目的にも利用できる。利用の日付、日時、利用者端末の識別、デジタルデータの識別、デジタルデータの転送経路の識別、利用の条件の記述等としても利用できる。

【0130】

【発明の効果】以上説明したように本発明によれば、デジタルデータに、そのデータのユーザ等に関する透かし

データを埋め込み、隠し持たせる電子透かし埋め込み装置において、複数のユーザが結託して互いのデータを比較したとしても、透かしデータを他のユーザに関する透かしデータに改竄することが困難とすることができる。

【図面の簡単な説明】

【図1】本発明による電子透かし埋め込み装置の第1の実施形態の構成を示すブロック図。

【図2】第1の実施形態の変形例の構成を示すブロック図。

【図3】図1中のデータ変換割当て部の詳細な構成を示すブロック図。

【図4】図1中のデータ変換割当て部の変形例のブロック図。

【図5】第1実施形態における識別符号の発生アルゴリズムを示すフローチャート。

【図6】第1実施形態における透かし検出装置の構成を示すブロック図。

【図7】第1実施形態の変形例における透かし検出装置の構成を示すブロック図。

【図8】第1実施形態における識別符号の復号のアルゴリズムを示すフローチャート。

【図9】本発明の第2実施形態における識別符号の発生アルゴリズムを示すフローチャート。

【図10】第2実施形態における識別符号の復号のアルゴリズムを示すフローチャート。

【図11】本発明の第3実施形態における識別符号の発生アルゴリズムを示すフローチャート。

【図12】第3実施形態における識別符号の復号のアルゴリズムを示すフローチャート。

【図13】本発明の第4実施形態における識別符号の発生アルゴリズムの前半を示すフローチャート。

【図14】本発明の第4実施形態における識別符号の発生アルゴリズムの後半を示すフローチャート。

【図15】本発明の第4実施形態における識別符号の復号のアルゴリズムの前半を示すフローチャート。

【図16】本発明の第4実施形態における識別符号の復号のアルゴリズムの後半を示すフローチャート。

【図17】本発明の第4実施形態の変形例における識別符号の発生アルゴリズムを示すフローチャート。

【符号の説明】

10…シンタックス解析部

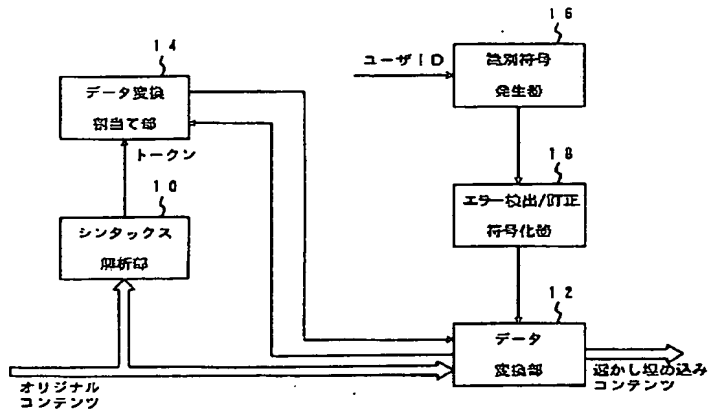
12…データ変換部

14…データ変換割当て部

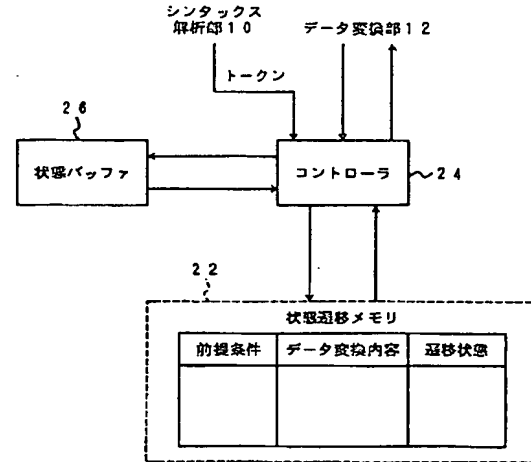
16…識別符号発生器

18…エラー検出／訂正符号化器

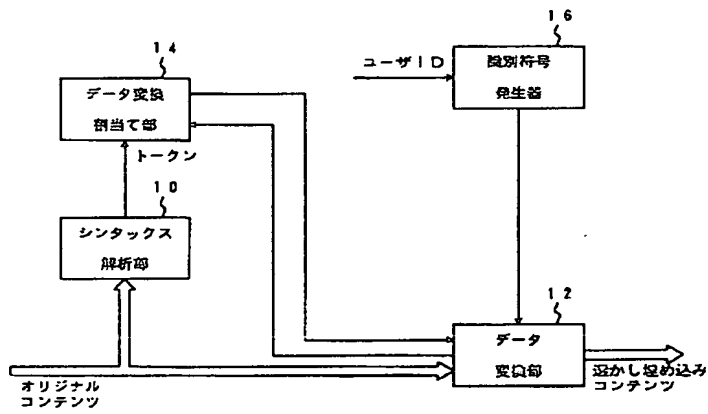
【図1】



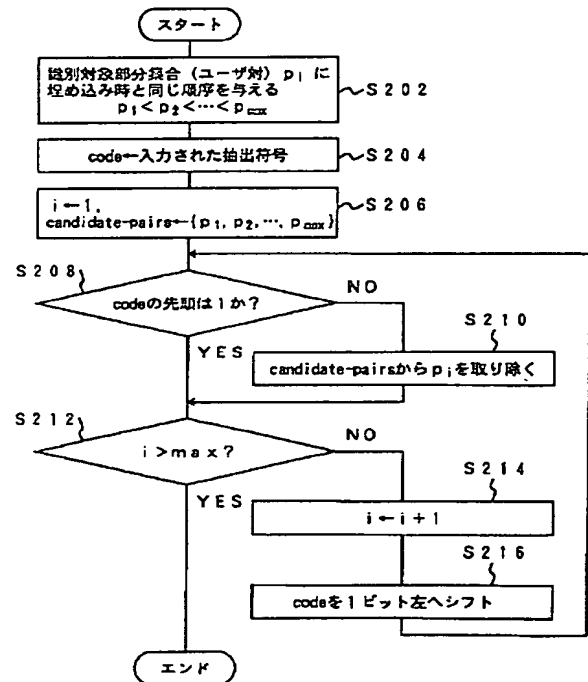
【図4】



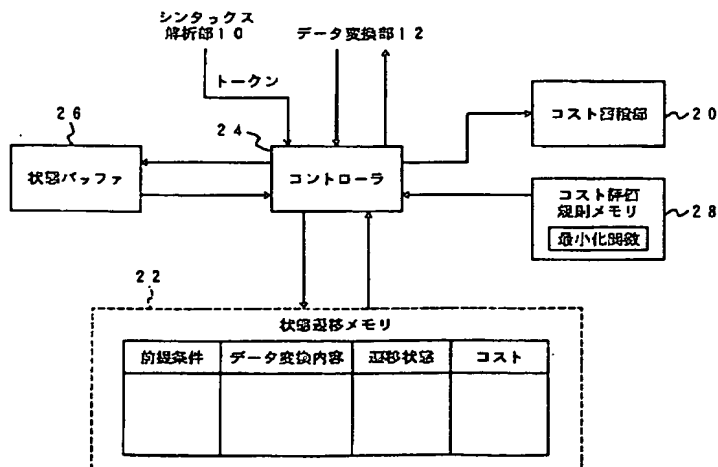
【図2】



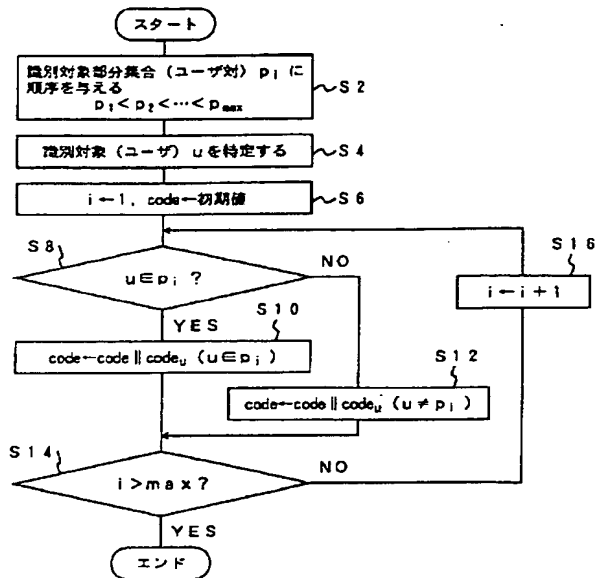
【図8】



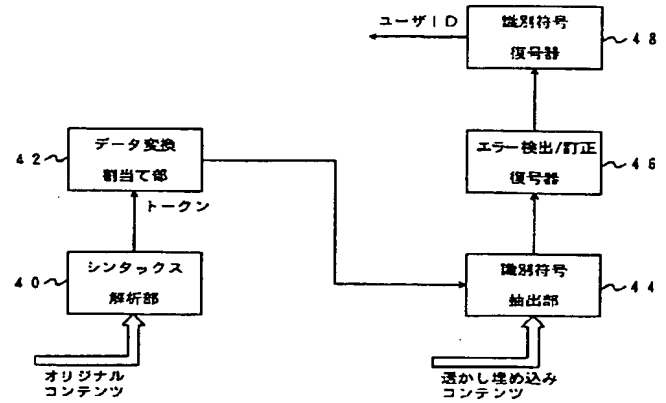
【図3】



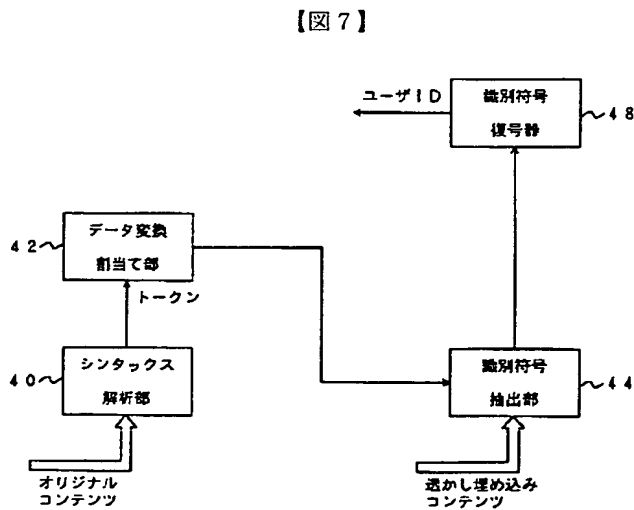
【図5】



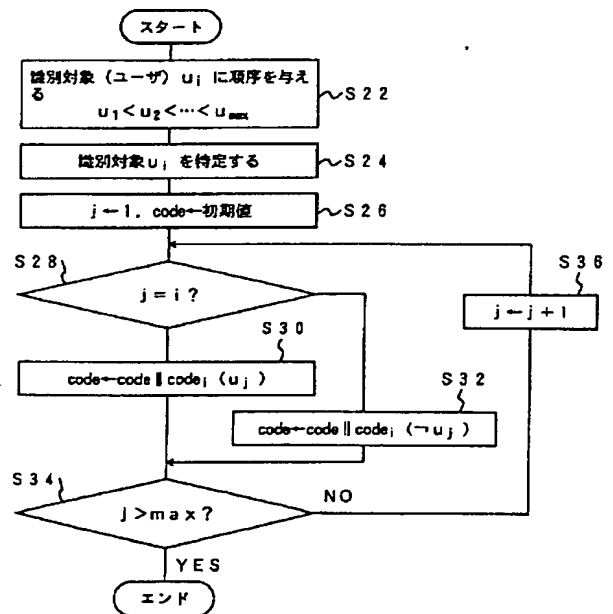
【図6】



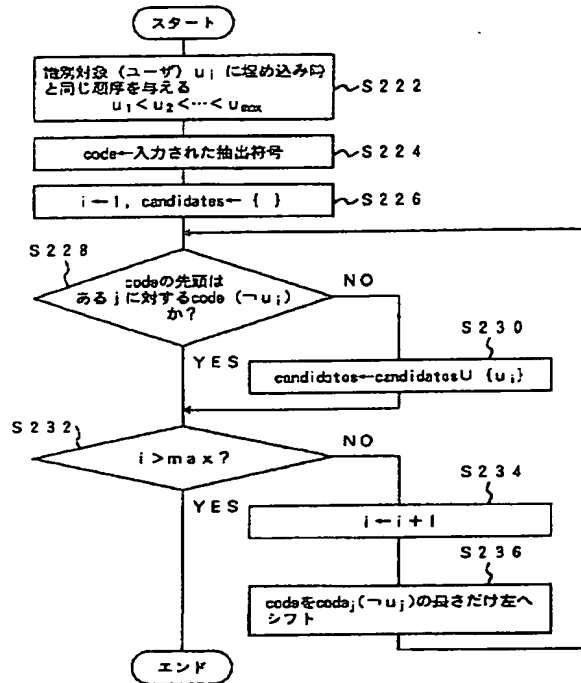
【図9】



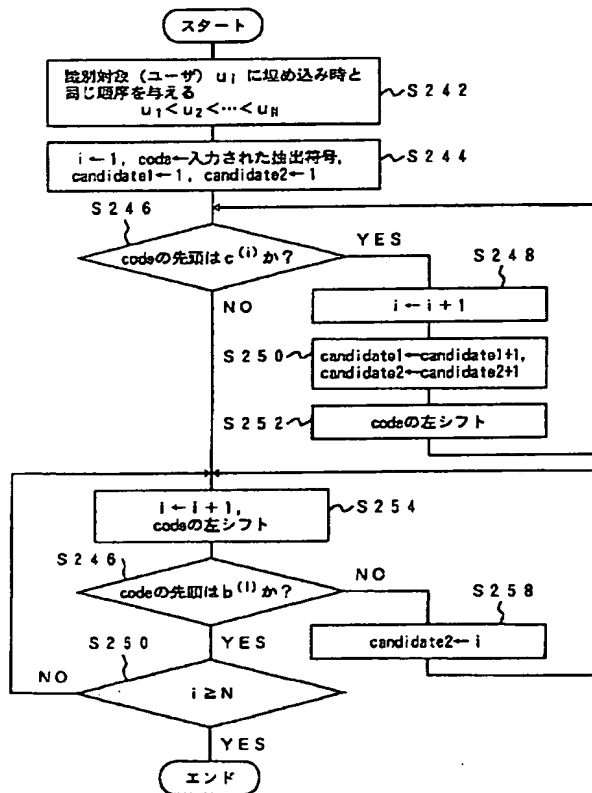
【図7】



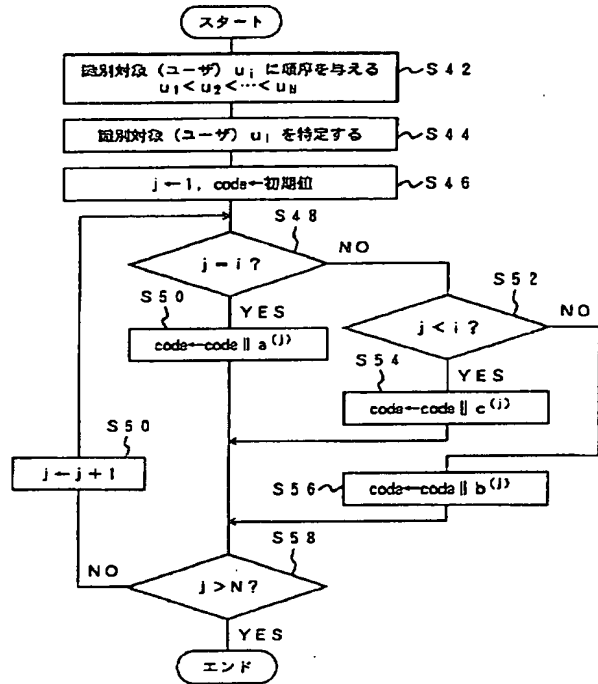
【図10】



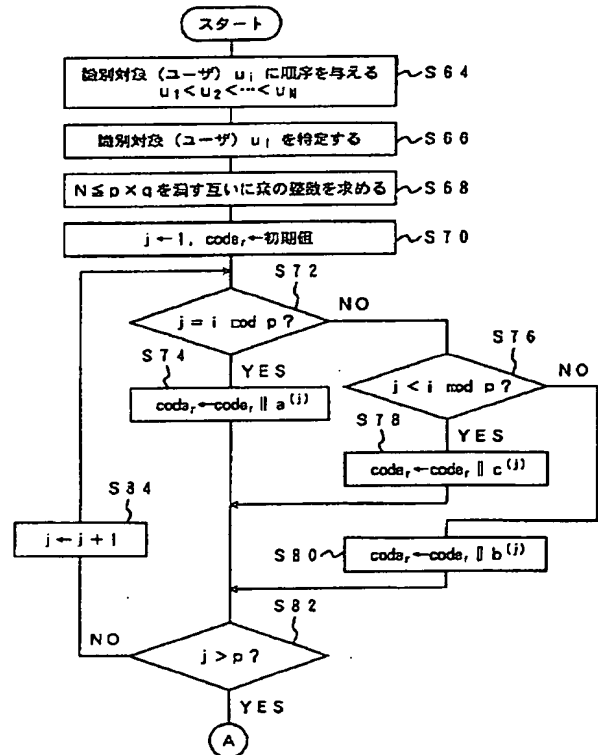
【図12】



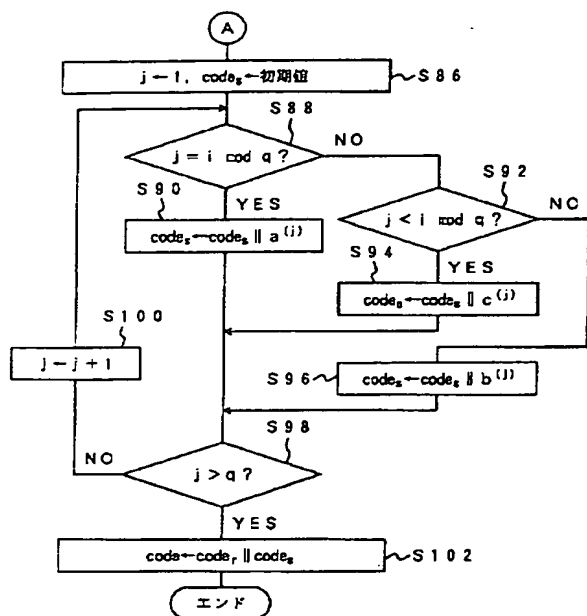
【図11】



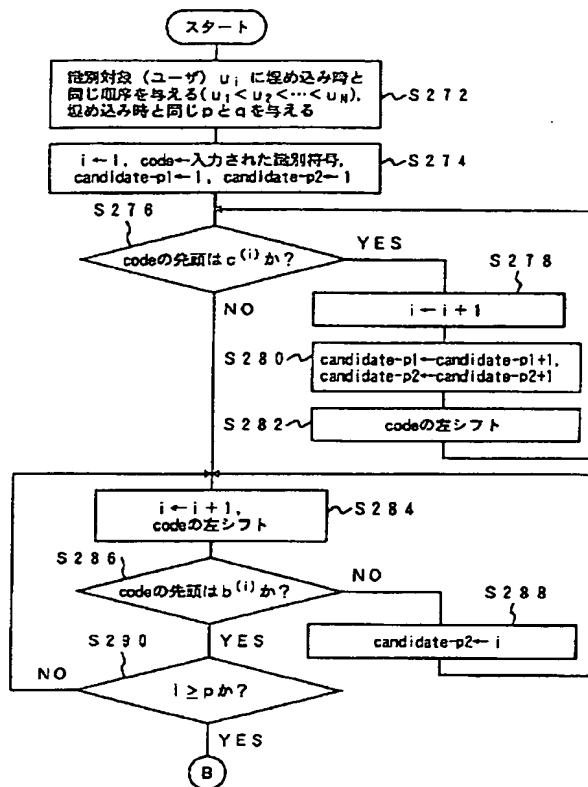
【図13】



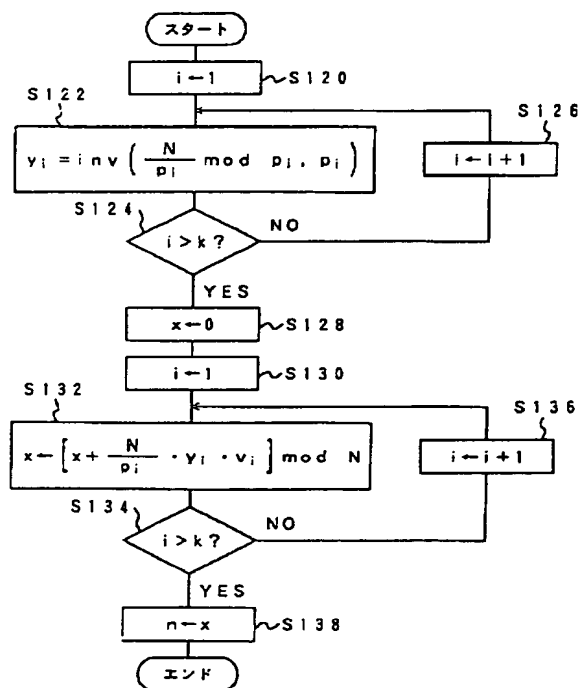
【図14】



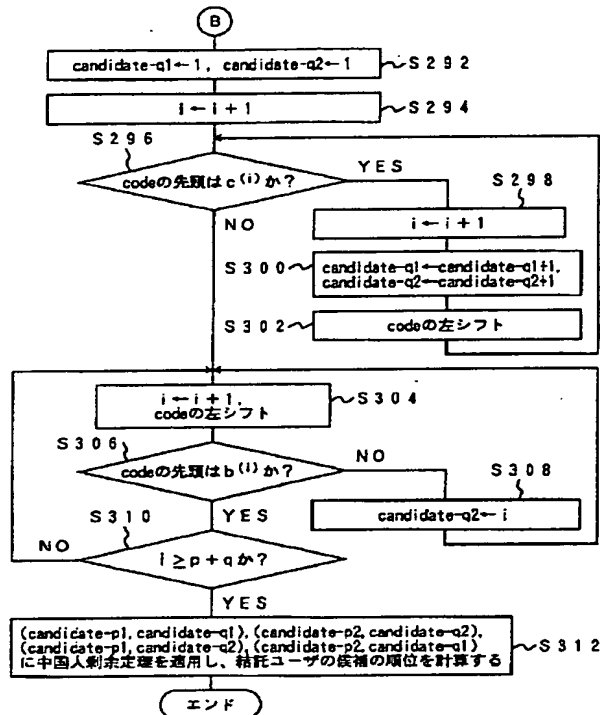
【図15】



【図17】



【図16】



【手続補正書】

【提出日】平成11年5月17日（1999. 5. 17）

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする電子透かし埋め込み装置。

【請求項2】 ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、当該ユーザがデジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を論理積の形で接続して用いることを特徴とする

電子透かし埋め込み装置。

【請求項3】 ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のあるユーザの各々に順位を付け、当該ユーザが各ユーザより順位が小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続して用いることを特徴とする電子透かし埋め込み装置。

【請求項4】 ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のあるユーザの各々に順位を付け、デジタルデータを渡す可能性のあるユーザの総数をNとし、 $N \leq p \times q$ となる互いに素の整数p、qそれぞれに対して、pを法とした当該ユーザの順位nの剰余が0からp-1までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報と、qを法とした当該ユーザの順位nの剰余が0からq-1までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報とをユ

ーザを識別する情報として用いることを特徴とする電子透かし埋め込み装置。

【請求項 5】 ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、全対象物の中の任意の 2 つの対象物の対の各々に対して、当該対象物がその対に含まれているか否かを表わす情報を発生することを特徴とする識別情報発生装置。

【請求項 6】 ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、当該対象物が全対象物の中の各対象物であるか否かを表わす情報を論理積の形で接続した情報を発生することを特徴とする識別情報発生装置。

【請求項 7】 ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、全識別対象物の各々に順位を付け、当該対象物が各識別対象物より順位が小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報を発生することを特徴とする識別情報発生装置。

【請求項 8】 全識別対象物の総数を N とし、 $N \leq p \times q$ となる互いに素の整数 p 、 q それぞれに対して、 p を法とした当該対象物の順位 n の剰余が 0 から $p-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報と、 q を法とした当該対象物の順位 n の剰余が 0 から $q-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報とを識別情報として発生することを特徴とする請求項 7 に記載の識別情報発生装置。

【請求項 9】 デジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容を記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、請求項 5 乃至請求項 8 のいずれか 1 項に記載の識別情報発生装置と、前記データ割当て部から出力されたデータ変換内容と前記識別情報発生装置から出力された識別情報に応じて、デジタルデータの所定の部分を変更する識別情報埋め込み手段と、を具備することを特徴とする識別情報埋め込み装置。

【請求項 10】 デジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容をその変化程度を表わすコストと共に記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、データ変換後のデータの変化程度を累積する手段と、請求項 5 乃至請求項 8 のいずれか 1 項に記載の識別情報

発生装置と、

前記データ割当て部から出力されたデータ変換内容と前記識別情報発生装置から出力された識別情報に応じて、デジタルデータの所定の部分を変更する識別情報埋め込み手段と、

前記累積手段により、データの変化程度の累積値が所定の変化程度を超える場合、前記識別情報埋め込み手段の動作を禁止する手段とを具備することを特徴とする識別情報埋め込み装置。

【請求項 11】 請求項 1 乃至請求項 4 のいずれか 1 項に記載の電子透かし埋め込み装置により、ユーザを識別する情報がユーザには知覚できないように符号化されて埋め込まれているデジタルデータから識別情報を読み取る識別情報検出装置において、デジタルデータの所定の位置に埋め込まれている識別符号を抽出する手段と、

抽出された識別符号を復号し、識別情報を求める手段と、

を具備することを特徴とする識別情報検出装置。

【請求項 12】 請求項 1 に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、デジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、その部位が請求項 1 に記載の装置により埋め込まれた、そのユーザ対がこのデジタルデータに対応するユーザを含んでいることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が請求項 1 に記載の装置により埋め込まれた、そのユーザ対がこのデジタルデータに対応するユーザを含んでいることを表わす符号であると判定されたユーザ対を結託したユーザ対の候補と推定することを特徴とする識別情報読取方法。

【請求項 13】 請求項 2 に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、デジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、その部位が請求項 2 に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザであることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が請求項 2 に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザであることを表わす符号であると判定されたユーザを結託したユーザの候補と推定することを特徴とする識別情報読取方法。

【請求項 14】 請求項 3 に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、

- 1) デジタルデータから抽出された識別情報から各ユーザに対応する部位を順次読み取るステップと、
- 2) その部位が請求項3に記載の装置により埋め込まれた、そのユーザの順位がこのデジタルデータに対応するユーザの順位よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ1)、2)を繰り返すステップと、
- 3) 上記ステップ2)において、初めて現れたそれ以外の符号の次の部位から、各ユーザに対応する部位を順次読み取るステップと、
- 4) その部位が請求項3に記載の装置により埋め込まれた、そのユーザの順位がこのデジタルデータに対応するユーザの順位よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ3)、4)を繰り返すステップと、
- 5) 抽出された識別情報の最後に到達するまで上記ステップ3)、4)、5)を繰り返すステップと、を具備し、
- 上記ステップ2)において、それ以外の符号が初めて現れた部位に対応するユーザを第一の結託ユーザ候補と推定し、
- 上記ステップ4)において、それ以外の符号が最後に現れた部位に対応するユーザを第二の結託ユーザ候補と推定することを特徴とする識別情報読取方法。

【請求項15】 請求項4に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、

- 1) デジタルデータから抽出された識別情報からpを法とするユーザのそれぞれに対応する部位を順次読み取るステップと、
- 2) その部位が、請求項4に記載の装置により埋め込まれた、pを法としたそのユーザの順位の剰余がpを法としたこのデジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ1)、2)を繰り返すステップと、
- 3) 上記ステップ2)において、初めて現れたそれ以外の符号を次の部位から、pを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
- 4) その部位が、請求項4に記載の装置により埋め込まれた、pを法としたそのユーザ順位の剰余がpを法としたこのデジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ3)、4)を繰り返すステップと、
- 5) 抽出された識別情報からpを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ3)、4)、5)を繰り返すステップと、

- 6) 上記ステップ5)において、抽出された識別情報からpを法としたユーザ順位の剰余のすべての部位を読み取った後、その次の部位からqを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
- 7) その部位が、請求項4に記載の装置により埋め込まれた、qを法としたそのユーザの順位の剰余がqを法としたこのデジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ6)、7)を繰り返すステップと、
- 8) 上記ステップ7)において、初めて現れたそれ以外の符号を次の部位から、qを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
- 9) その部位が、請求項4に記載の装置により埋め込まれた、qを法としたそのユーザ順位の剰余がqを法としたこのデジタルデータに対応するユーザ順位の剰余よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ8)、9)を繰り返すステップと、
- 10) 抽出された識別情報からqを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ8)、9)、10)を繰り返すステップと、を具備し、上記ステップ2)において、それ以外の符号が初めて現れた部位に対応するpを法としたユーザ順位の剰余と、上記ステップ4)において、それ以外の符号が最後に現れた部位に対応するpを法としたユーザ順位の剰余と、上記ステップ7)において、それ以外の符号が初めて現れた部位に対応するqを法としたユーザ順位の剰余と、上記ステップ9)において、それ以外の符号が最後に現れた部位に対応するqを法としたユーザ順位の剰余とを組み合わせる構成されるpを法とする剰余とqを法とする剰余の組に対して中国人剰余定理を適用して結託ユーザの候補を推定することを特徴とする識別情報読取方法。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

【補正内容】

【0017】

【発明が解決しようとする課題】このように従来の電子透かし埋め込み技術は、ユーザを識別する透かしデータを当該ユーザには知覚できない状態で埋め込み、隠し持たせることができるが、複数のユーザが結託してデータを互いに比較することにより、透かしデータが埋め込まれている位置に関する情報を得ることができてしまい、透かしデータの偽造や消去を容易にするという欠点があった。また、結託したユーザを特定できるような識別情報の埋め込み法もあるが、結託に参加したユーザが2人の場合しか特定できず、3人以上のユーザが結託した場合

合は、特定できない欠点がある。また、必ずしも結託ユーザを特定できない場合もあり、結託ユーザを特定できる確率が低かった。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正内容】

【0018】本発明の目的は、複数のユーザが結託して互いのデータを比較したとしても、埋め込まれている透かしデータに関する情報を十分に得ることができず、透かしデータを偽造や消去することが困難となるように、デジタルデータに、そのデータのユーザ等に関する透かしデータを埋め込み、隠し持たせることができ、しかも3人以上のユーザが結託して透かしデータを改竄した場合でも、高い確率で結託したユーザを特定できる電子透かし埋め込み装置を提供することである。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0020

【補正方法】変更

【補正内容】

【0020】(1) ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のある全ユーザの中の任意の2人のユーザ対の各々に対して、当該ユーザがその対に含まれているか否かを表わす情報を用いることを特徴とする。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0021

【補正方法】変更

【補正内容】

【0021】(2) ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、当該ユーザがデジタルデータを渡す可能性のある各ユーザであるか否かを表わす情報を論理積の形で接続して用いることを特徴とする。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0022

【補正方法】変更

【補正内容】

【0022】(3) ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のあるユーザの各々に順位を付け、当該ユーザが各ユーザよ

り順位が小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続して用いることを特徴とする。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0023

【補正方法】変更

【補正内容】

【0023】(4) ユーザに渡すデジタルデータにユーザを識別する情報を、ユーザには知覚できないように埋め込む電子透かし埋め込み装置において、ユーザを識別する情報として、デジタルデータを渡す可能性のあるユーザの各々に順位を付け、デジタルデータを渡す可能性のあるユーザの総数を N とし、 $N \leq p \times q$ となる互いに素の整数 p 、 q それぞれに対して、 p を法とした当該ユーザの順位 n の剰余が0から $p-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報と、 q を法とした当該ユーザの順位 n の剰余が0から $q-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報とをユーザを識別する情報として用いることを特徴とする。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0024

【補正方法】変更

【補正内容】

【0024】(5) ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、全対象物の中の任意の2つの対象物の対の各々に対して、当該対象物がその対に含まれているか否かを表わす情報を発生することを特徴とする。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0025

【補正方法】変更

【補正内容】

【0025】(6) ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、当該対象物が全対象物の中の各対象物であるか否かを表わす情報を論理積の形で接続した情報を発生することを特徴とする。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0026

【補正方法】変更

【補正内容】

【0026】(7) ある対象物を識別する識別情報を発生する識別情報発生装置において、識別情報として、全識別対象物の各々に順位を付け、当該対象物が各識別対

象物より順位が小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報を発生することを特徴とする。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0027

【補正方法】変更

【補正内容】

【0027】(8) 全識別対象物の総数を N とし、 $N \leq p \times q$ となる互いに素の整数 p 、 q それぞれに対して、 p を法とした当該対象物の順位 n の剰余が0から $p-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報と、 q を法とした当該対象物の順位 n の剰余が0から $q-1$ までのそれぞれに対して小さいか、等しいか、あるいは大きいかを表わす情報を論理積の形で接続した情報とを識別情報として発生することを特徴とする。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0028

【補正方法】変更

【補正内容】

【0028】(9) デジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容を記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、(5)乃至(8)のいずれかに記載の識別情報発生装置と、前記データ割当て部から出力されたデータ変換内容と前記識別情報発生装置から出力された識別情報に応じて、デジタルデータの所定の部分を変更する識別情報埋め込み手段と、を具備することを特徴とする識別情報埋め込み装置。

【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0029

【補正方法】変更

【補正内容】

【0029】(10) デジタルデータをシンタックス解析し、ある意味を持ったひとかたまりのデータ毎に、その意味を示すトークンに関する情報を出力するシンタックス解析部と、種々のデータ変換内容をその変化程度を表わすコストと共に記憶しており、トークンに応じてデータ変換内容を出力するデータ変換割当て部と、データ変換後のデータの変化程度を累積する手段と、(5)乃至(8)のいずれかに記載の識別情報発生装置と、前記データ割当て部から出力されたデータ変換内容と前記識別情報発生装置から出力された識別情報に応じて、デジタルデータの所定の部分を変更する識別情報埋め込み手段と、前記累積手段により、データの変化程度の累

積値が所定の変化程度を超える場合、前記識別情報埋め込み手段の動作を禁止する手段とを具備することを特徴とする識別情報埋め込み装置。

【手続補正14】

【補正対象書類名】明細書

【補正対象項目名】0030

【補正方法】変更

【補正内容】

【0030】(11) (1)乃至(4)のいずれかに記載の電子透かし埋め込み装置により、ユーザを識別する情報がユーザには知覚できないように符号化されて埋め込まれているデジタルデータから識別情報を読み取る識別情報検出装置において、デジタルデータの所定の位置に埋め込まれている識別符号を抽出する手段と、抽出された識別符号を復号し、識別情報を求める手段と、を具備することを特徴とする。

【手続補正15】

【補正対象書類名】明細書

【補正対象項目名】0031

【補正方法】変更

【補正内容】

【0031】(12) (1)に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、デジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、その部位が(1)に記載の装置により埋め込まれた、そのユーザ対がこのデジタルデータに対応するユーザを含んでいることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が(1)に記載の装置により埋め込まれた、そのユーザ対がこのデジタルデータに対応するユーザを含んでいることを表わす符号であると判定されたユーザ対を結託したユーザ対の候補と推定することを特徴とする。

【手続補正16】

【補正対象書類名】明細書

【補正対象項目名】0032

【補正方法】変更

【補正内容】

【0032】(13) (2)に記載の電子透かし埋め込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、デジタルデータから抽出された識別情報から各ユーザ対に対応する部位を読み取るステップと、その部位が(2)に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザであることを表わす符号であるか、それ以外の符号であるかを判定するステップとを具備し、その部位が(2)に記載の装置により埋め込まれた、そのユーザがこのデジタルデータに対応するユーザであることを表わす符号であると判定

されたユーザを結託したユーザの候補と推定することを特徴とする。

【手続補正17】

【補正対象書類名】明細書

【補正対象項目名】0033

【補正方法】変更

【補正内容】

【0033】(14) (3)に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、
1) デジタルデータから抽出された識別情報から各ユーザに対応する部位を順次読み取るステップと、
2) その部位が請求項3に記載の装置により埋め込まれた、そのユーザの順位がこのデジタルデータに対応するユーザの順位よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ1)、2)を繰り返すステップと、
3) 上記ステップ2)において、初めて現れたそれ以外の符号の次の部位から、各ユーザに対応する部位を順次読み取るステップと、
4) その部位が(3)に記載の装置により埋め込まれた、そのユーザの順位がこのデジタルデータに対応するユーザの順位よりの大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ3)、4)を繰り返すステップと、
5) 抽出された識別情報の最後に到達するまで上記ステップ3)、4)、5)を繰り返すステップと、を具備し、上記ステップ2)において、それ以外の符号が初めて現れた部位に対応するユーザを第一の結託ユーザ候補と推定し、上記ステップ4)において、それ以外の符号が最後に現れた部位に対応するユーザを第二の結託ユーザ候補と推定することを特徴とする。

【手続補正18】

【補正対象書類名】明細書

【補正対象項目名】0034

【補正方法】変更

【補正内容】

【0034】(15) (4)に記載の電子透かし埋込み装置により、ユーザを識別する情報が埋め込まれたデジタルデータから識別情報を読み取る方法において、
1) デジタルデータから抽出された識別情報からpを法とするユーザのそれぞれに対応する部位を順次読み取るステップと、
2) その部位が、(4)に記載の装置により埋め込まれた、pを法としたそのユーザの順位の剰余がpを法としたこのデジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ス

テップ1)、2)を繰り返すステップと、

3) 上記ステップ2)において、初めて現れたそれ以外の符号を次の部位から、pを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、
4) その部位が、(4)に記載の装置により埋め込まれた、pを法としたそのユーザ順位の剰余がpを法としたこのデジタルデータに対応するユーザ順位の剰余より大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ3)、4)を繰り返すステップと、

5) 抽出された識別情報からpを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ3)、4)、5)を繰り返すステップと、

6) 上記ステップ5)において、抽出された識別情報からpを法としたユーザ順位の剰余のすべての部位を読み取った後、その次の部位からqを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

7) その部位が、(4)に記載の装置により埋め込まれた、qを法としたそのユーザの順位の剰余がqを法としたこのデジタルデータに対応するユーザ順位の剰余よりも小さいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ6)、7)を繰り返すステップと、

8) 上記ステップ7)において、初めて現れたそれ以外の符号を次の部位から、qを法としたユーザ順位の剰余のそれぞれに対応する部位を順次読み取るステップと、

9) その部位が、(4)に記載の装置により埋め込まれた、qを法としたそのユーザ順位の剰余がqを法としたこのデジタルデータに対応するユーザ順位の剰余より大きいことを表す符号であるか、それ以外の符号であるかを判定し、それ以外の符号が現れるまで、上記ステップ8)、9)を繰り返すステップと、

10) 抽出された識別情報からqを法としたユーザ順位のすべての部位を読み取るまで、上記ステップ8)、9)、10)を繰り返すステップと、を具備し、上記ステップ2)において、それ以外の符号が初めて現れた部位に対応するpを法としたユーザ順位の剰余と、上記ステップ4)において、それ以外の符号が最後に現れた部位に対応するpを法としたユーザ順位の剰余と、上記ステップ7)において、それ以外の符号が初めて現れた部位に対応するqを法としたユーザ順位の剰余と、上記ステップ9)において、それ以外の符号が最後に現れた部位に対応するqを法としたユーザ順位の剰余とを組み合わせ

て構成されるpを法とする剰余とqを法とする剰余の組に対して中国人剰余定理を適用して結託ユーザの候補を推定することを特徴とする。

【手続補正19】

【補正対象書類名】明細書

【補正対象項目名】0086

【補正方法】変更

【補正内容】

【0086】（第3実施形態）第2実施形態は上述の符号を用いる場合は、3人以上のユーザの結託には弱い。結託者が3人以上の場合には、例えば多数決攻撃（互いの差分のデータ“0”、“1”を多数のデータに書き換える）を行うことによって、どのユーザをも表さない連接された符号を偽造できる。しかし、ユーザaでないことをあらわす符号を複数用意することによって、多数決攻撃は有効でなくなる。なぜなら、ユーザaでないとい

う符号が複数存在するので多数決によっては、ユーザaでないという符号を得ることができないからである。

【手続補正20】

【補正対象書類名】明細書

【補正対象項目名】0087

【補正方法】変更

【補正内容】

【0087】上述のようにユーザaではないという符号を1個しか用いない場合の第2実施形態において、ユーザu_i、u_j、u_kが結託する場合を考える。

